Rough Draft **DA PAM 25-IA**
August 1999 Edition

Information Assurance Implementation Guide

HQDA-DISC4
WASHINGTON, DC

(NOTE --- NOTE: CHAPTER 1 THRU PARAGRAPH 2-4, CHAPTER 2 DEVELOPED BY DA PAM COMMITTEE # 1)

CHAPTER 1: GENERAL POLICY

History. This is a new publication. This pamphlet is published as implementing procedures for the new regulation, AR25-IA, Information Assurance. Proponency for this pamphlet and companion regulation is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4).

Summary. This DA PAM provides specific guidance for AR25-IA compliance. It establishes procedures for implementing the Army Information Assurance Program (AIAP).

Applicability. This pamphlet applies to the Active Army, the Army National Guard (ARNG), the U.S. Army Reserve (USAR), its agents and contractors.

Proponent and exception authority. The proponent for this pamphlet is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4). The proponent has the authority to approve exceptions to this pamphlet that have received a legal review to ensure that the exception is consistent with controlling law and regulation. The proponent may delegate the approval authority, in writing, to a division chief within the proponent agency in the grade of colonel or the civilian equivalent.

Army Management Control Process. This pamphlet contains management control provisions that are contained in AR 25-IA and it identifies key management controls that must be evaluated. A management Control Evaluation Checklist is located in Appendix B.

Interim changes. Interim changes to this pamphlet are not official until they are authenticated by the Administrative Assistant to the Secretary of the Army. Users shall destroy interim changes on their expiration dates, unless sooner superseded or rescinded.

Supplementation. Major Commands may supplement this pamphlet. Copies of all supplements must be forwarded to Director of Information Systems for Command, Control, Communications, and Computers (DISC4), 107 Army, Pentagon, Washington DC 20310-107, for concurrence and legal review prior to implementation.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Director of Information Systems for Command, Control, Communications, and Computers (DISC4), 107 Army Pentagon, Washington DC 20310-107.

Mobilization status. During mobilization, deployment, or national emergency, this pamphlet remains in effect without change.

Distribution. Distribution of this publication is made in accordance with the requirements of DA Form 1209 E, block 5066 intended for command level B, C, D, and E for the Active Army, the Army National Guard, the Army Reserve, its agents and contractors. Chapter 1 Introduction

1-1. PURPOSE.
Information Assurance (IA) is the component of Information Operations that assures DOD's operational readiness by providing for the continuous availability and reliability of information systems and networks. IA protects the Defense Information Infrastructure (DII) against exploitation, degradation, and denial of service, while providing the means to efficiently reconstitute and reestablish vital capabilities following an attack. The Army Information Assurance Program (AIAP)

outlines the measures that Army Leadership must undertake to ensure that the Army's portion of the Defense Information Infrastructure (DII) is adequately protected. It specifically addresses the IA sub-disciplines of communications security (COMSEC) and computer security (COMPUSEC). This pamphlet is published as implementing procedures for the new regulation, AR25-IA, Information Assurance, provides the following:

a. Procedures for the security and protection of systems that create, process, store, and transmit SBU, classified and caveated/handling coded information.

b. Procedures and systems security requirements, including those for interconnected systems.

c. Training and Certification requirements for IA and Information Systems (IS) personnel.

d. The use of risk assessment procedures.

e. The Certification and Accreditation process as well as levels of concern and protection.

f. The Network Security Improvement Plan (NSIP).

g. Procedures as they apply to:

(1) Hardware

(2) Software

(3) Firmware

(4) Telecommunications

(5) Personnel

(6) Physical Environment

(7) Networks

1-2. References. Required and related publications and referenced forms are listed in Appendix A.

1-3. Abbreviations and Terms. Explanation of abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities. Specific duties and responsibilities for the positions listed below are identified in paragraph 1-4, AR 25-IA.

a. The Assistant Secretary of the Army for Research, Development, and Acquisition (ASARDA).

b. Director of Information Systems for Command, Control, Communications and Computers (DISC4).

c. The HQDA, Deputy Chief of Staff for Intelligence (DCSINT).

d. The Deputy Chief of Staff for Operations and Plans (DCSOPS).

e. The Deputy Chief of Staff for Logistics (DCSLOG).

f. The U. S. Army Audit Agency.

(1) The USAAA will perform audit assistance work for audit organizations internal and external to DA. Requests for audit assistance will generally be approved providing the work can be performed within available resources, and interference with the primary Agency mission will be minimal. Requests will normally be in writing and should clearly state the purpose and scope of assistance desired. Requests for normal or limited scope audits from the Army Secretariat, DA Staff, and major commanders or field commanders will be addressed to The Auditor General. Requests for audit assistance must be forwarded and approved by The Auditor General or Regional Deputy Auditors General.

(2) Work with HQDA proponents, major commands, installations and technical experts (e.g., Land Information Warfare Activity (LIWA)) on IA issues through engagement letters, memorandums of agreements, operations and IAW AR 36-5.

(3) Conduct entrance and exit conferences. The commander or head of the audited activity should attend the entrance and exit conferences to coordinate audit schedules and objectives and exchange information to help meet audit objectives and goals, to include actual or target completion dates.

(4) Recommend corrective action to “Serious incidents", per AR 190-40, involving abuse, illegal activity, or statutory violations that in the auditors' opinion require immediate action. If the audited activity agrees with the recommendations, corrective actions will be initiated promptly.

(5) Agency audit reports will not be released to any individual or organization outside the Agency without obtaining proper chain of approval, other than the distribution contained in the printed audit report (the annex titled "Others Receiving Copies of the Report").

(6) Release of audit reports under the Freedom of Information Act will be made by the USAAA Office of Counsel in accordance with the procedures contained in USAAA Regulation 27-1 and pertinent Army regulations.

g. Land Information Warfare Activity (LIWA).

h. Commanders of Major Army Commands (MACOMs), Chief, Army Reserve (CAR), Chief, National Guard Bureau (NGB), Program Executive Officers (PEO) and the Administrative Assistant to the Secretary of the Army (acting as the MACOM for all HQDA staff agencies).

ADD INFO ON IA TRIAD MISSION.

i. In addition to the duties and responsibilities as MACOMs, the following Commanders have specific responsibilities as outlined in para 1-4, AR 25-IA:

(1) The Commanding General, U.S. Army Forces Command (FORSCOM), in addition to the MACOM responsibilities listed above, shall exercise command and control of the U.S. Army Signal Command (USASC).

(2) Commanding General, US Army Training and Doctrine Command (TRADOC).

(3) Commanding General, US Army Materiel Command (AMC).

(4) Commanding General, US Army Intelligence and Security Command (INSCOM).

j. Program Executive Officers (PEOs) and Program/Project Managers (PMs).

k. Commanders, Directors and Managers (at all levels below MACOM) responsible for implementing the AIAP in their command or activity.

l. Host and Tenant Responsibilities.

(1) Installation/Host IAM shall draw up a formal Memorandum of Agreement (MOA) identifying:

(a) The specifics of tenant connectivity (i.e., use of the installation backbone, routers or gateways)

(b) IA security requirements established by the Host (e.g., incident reporting requirements and configuration management).

(2) Tenant IAM shall identify IS and provide an approved accreditation document to the Host/Installation for enclosure in the Host Accreditation statement.

1-5. IA Structure. IA personnel shall be appointed on orders (see FIGURE 1-1) to implement the Army Information Assurance Program (AIAP) (Table 1-1). Appointment orders will not exceed two (2) years in duration, however individuals may be re-appointed an unlimited number of times. Special instructions for appointment orders will include "The individual has the authority to enforce security policies and safeguards for systems within their purview. This authority includes halting system operations if warranted by the impact of a security deficiency." The IA staff will be optimally positioned organizationally to avoid having a vested interest in keeping the system operational at the expense of security.

a. The following IA positions exist at the MACOM Level:

(1) Information Assurance Program Manager (IAPM).

(2) Information Assurance Network Manager (IANM).

b. The following IA positions exist at the MSC / Installation Level:

(1) Information Assurance Manager (IAM).

2) Information Assurance Network Manager / Officer (IANM/O).

c. The following IA positions exist at the Unit / Organizational Level:

(1) Information Assurance Security Officer (IASO).

Table 1-1. Information Assurance Personnel Requirements

		LOCATION			Security Clearance Requirements (AR380-67)		
Position	Rank / Grade	MACOM	MSC/Installation	Unit/Organization	ADP I	ADP II	ADP III
IAPM	LTC / GS14	X			X		
IANM	MAJ / GS13 / CW3	X			X		
IAM	*		X			X	
IANM/O	*		X			X	
IASO	*			X			X

* Denotes Local Policy

Office Symbol (25-IA) (Date)

MEMORANDUM FOR RECORD

SUBJECT: Appointment of (IA position title)

1. Effective (date), (name of individual), (SSN), is appointed as (IA position title).

2. Authority: AR 25-IA, para 1-5.

3. Purpose: To serve as (IA position title) for (unit /organization and system, if applicable).

4. Special Instructions: Individual has the authority to enforce security and safeguards for systems within their purview. This authority includes halting system operations if warranted by the impact of a security deficiency.

5. Period: This appointment expires two years from the effective date.

(Signature block of Commander or Director)

CF:
Individual Concerned
(additional distribution, as needed)

FIGURE 1-1 IA APPOINTMENT ORDERS

CHAPTER 2, INFORMATION SYSTEMS SECURITY

Section I
General Policy

2-1. Overview. All Army Information Assurance Programs must include security analyses, security engineering, and security countermeasures to detect, respond, react and report within the broad constraints of cost-effectiveness and adherence to public laws, DOD Directives, and Army Regulations.

a. IA funding. Operations and Maintenance , Army (OMA) and Operations and Maintenance, Army Reserve (OMAR) funding to support ISS initiatives is provided by HQDA to the MACOMs in Management Decision Package (MDEP) MS4X and MX5T (MX5T is used for COMSEC, AR 380-40 & 380-53). IA initiatives are those associated with the security and protection of IS against espionage, sabotage, misuse, fraud, theft, and denial of service. MDEP MS4X funds will not be reprogrammed without prior approval of the ODISC4.

b. MS4X Funding. MACOMs will establish command priority for execution of MDEP MS4X funds. Authorized MDEP MS4X expenditures include, but are not limited to, IA-related initiatives such as:

(1) Training. TDY and tuition costs for IA-related training, seminars and conferences (commercial or government provided) and to conduct IA oversight, compliance, or assistance visits.

(a) Security education and awareness training for end users, management personnel, and IA personnel.

(b) Systems and network administrator training.

(c) Department of Defense Information Intelligence Systems (DODIIS) training.

(2) Equipment.

(a) Security products, systems or accessories, e.g., firewalls, intrusion detection systems, computer security cable kits/locks.

(b) Computers/printers to support classified processing requirements.

(c) Hardware, e.g., removable disk drives and tape backup systems, power/surge protectors.

(d) Security software.

(3) Salaries.

(a) Contract for service of IA related support(Contractor personnel).
(b) Permanent and temporary (Government Employees).

c. MS4X funds cannot be used for:

(1) Awards

(2) Non-IA related supplies, computers, hardware, software (e.g. printers, scanners).

(3) Non-IA related training.

(4) Non-IA related service and maintenance contracts.

(5) Equipment, support or training for joint or non-army systems.

(6) Shredders.

(7) Secure Telephone Units (STUs)

(8) Cell phones.

(9) Facsimile machines.

(10) Copy machines.

(11) Video equipment.

(12) Communications equipment.

(13) Furniture
(NOTE: Expenditure is authorized for items 6-12 if specifically dedicated to IA Program)

d. Reporting Requirements. (RCS:?????) All MACOMs will provide the following MDEP MS4X reports (figure 1-2) to the HQDA, DISC4, ATTN: SAIS-IAS

(1) FY phased execution plan must be submitted to the DISC4 no later than 10 Aug of each year.

(2) Actual Execution Reports. Funded commands must provide a detailed mid-year and year-end actual execution report.

(a) The mid-year actual execution report is due to the DISC4 not later than 10 May of each fiscal year.

(b) The year-end actual execution report is due to the DISC4 not later than 10 Oct of each fiscal year.

(c) Both the mid-year and year-end actual execution reports must be (1) tied to phased execution plans and (2) reconciled with official Execution Database Summary (218) report.

(3) Execution reports will be reviewed for unauthorized expenditures and unauthorized fund reprogramming.

e. MX5T – EQUIPMENT REQUIREMENTS (DISC4)

f. CSLA – ISSP DATA BASE (DISC4)

g. Minimum execution standards for MS4X and MX5T are established in AR 25-IA, paragraph 2-1m(2).

h. Submission of Unresourced Requirements will be to DISC4, SAIS-IAS.

MDEP MS4X, INFORMATION ASSURANCE
PHASED FUNDING UTILIZTION PLAN/ACTUAL EXECUTION REPORT (RCS:)
For period ending _____ (MMYY)

	Phased Fund Utililization Plan				
Project Exection Data (MM/YY)	ITEM (e.g., training (what type and # of participants); specific equipment items)	EST. COST ($000)	ACT. OBL ($000)	DATE OBL ($000) (MM/YY)	REMARKS: (e.g., status o execution of funds in line v

2-2. IA Training. All individuals who are appointed as IAPMs, IAMs, IANMs, IANM/Os and IASOs must complete an IA security course of instruction equal to the duties assigned to them. All other personnel who manage, design, develop, maintain, or operate IS will undergo a training and awareness program. System Administrators and Network Managers must also complete certification training.

a. IA personnel listed in Paragraph 1-5 IA Structure, must complete one of the classroom courses listed below:

(1) INFOSEC 300 (INFOSEC for ISSOs/ISSMs)

(2) ND-225 (Operational Computer Security)

(3) ISSB (Information System Security basics)

(4) Equivalent Courses as designated by DISC4 (e.g., AMEC 305, ISS for Managers)

(5) Physical and environmental considerations that are necessary to protect the system.

(6) System data and access controls.

(7) Emergency and disaster plans.

(8) Authorized systems configuration and associated configuration management requirements.

c. Periodic security training and awareness, which may include various combinations of the following:

(1) Self paced or formal instruction.

b. An Initial security training and awareness briefing for IA Managers and users. This briefing can consist of training material governing IA in general but must be tailored to the system the employee will be managing or using. The briefing will include the following:

(1) Threats, vulnerabilities, and risks associated with the system. Under this portion, specific information regarding measures to reduce the threat from malicious software will be provided, including prohibitions on loading unauthorized software, the need for frequent backup, and the requirement to report abnormal program or system behavior immediately.

(2) Information security objectives (that is, what is it that needs to be protected).

(3) Responsibilities and accountability associated with IA.

(4) Information accessibility, handling, and storage considerations.

(2) Security information bulletins.

(3) Security posters.

(4) Training films and tapes.

(5) Computer-aided instruction.

d. In addition to the courses identified above, System Administrators and Network Managers must complete certification training as identified below.

(1) Level I – CD-ROMs: InfoSec Awareness and Operational Information Systems Security, Volume 1 and Volume 2.

(2) Level II – Classroom Studies: Systems Administrators Security Course and/or Network Managers Security Course.

(3) Level III – To Be Determined by DISC4.

2-3 Levels of Concern and Protection Levels.

a. Levels-of-Concern. The DAA, using guidance from the Data Owner, and after examining the information characteristics of the IS in question, must determine the appropriate Levels-of-Concern ratings for confidentiality, integrity, and availability. The Level-of-Concern rating for each of these areas can be either Basic, Medium, or High. The Level-of-Concern rating is independent for each of these three areas.

(1)The decision regarding the Levels-of-Concern shall be explicit for all (including interconnected) systems. The record of this decision shall be written, and the DAA shall ensure that these records are retained for the operational life of the system(s) involved. At the DAA's discretion, the decision can be made for groups of systems, but it shall be explicit.

(2) Table 3.1 of DCID 6/3 is designed to assist those involved in system development, implementation, certification, and accreditation in determining the appropriate Levels-of-Concern for confidentiality, integrity and availability for a given system processing a given set of information.

b. Protection Levels. The concept of Protection Levels applies only to confidentiality., the DAA must next ascertain the appropriate Protection Level for the IS based on the required clearance(s), formal access approval(s), and need-to-know of all direct and indirect users who receive information from the IS without manual intervention and reliable human review after having verified that an IS will maintain, process, or transmit intelligence information and therefore that its Level of Concern for confidentiality must be High. It indicates an implicit level of trust that is placed in the system's technical capabilities.

(1) The DAA must also assign a Protection Level to each IS that is to be accredited. The decision regarding the Protection Levels shall be explicit for all (including interconnected) systems. The record of this decision shall be in writing, and the DAA shall ensure that these records are retained for the operational life of the system(s) involved. At the DAA's discretion, the decision can be made for groups of systems, but it shall be explicit.

(2) Table 4.1 of DCID 6/3 identifies the criteria for determining which of the five Protection Levels is appropriate for the IS being accredited.

2-4. Minimum Requirements. Commanders and accreditation authorities may impose more stringent requirements based on a risk analysis. All risk analyses will evaluate the possible vulnerabilities and the security impact on the associated IS and networks within the area of responsibility. Although manual procedures are acceptable when an automated safeguard is not feasible, security safeguards will be imbedded into design of IS to ensure a secure infrastructure.

a. Accountability. For all AIS except small computers (see glossary), a security audit trail will provide a documented history of IS use. In a client server environment (CSE), audits will be maintained at the server level. The audit trail will be sufficient to reconstruct events in determining the cause or magnitude of compromise or damage should a security violation or malfunction occur. Audit trails will be reviewed once per week as a minimum. The DAAs will determine how long to retain the audit information.

b. Audit. The security audit trail will document the following:

(1) The identity of each person and device accessing the IS.

(2) The date and time of the access.

(3) User activity sufficient to ensure user actions are controlled and open to scrutiny.

(4) Activities that might modify, bypass, or negate safeguards controlled by the AIS.

(5) Security relevant actions associated with periods of processing or the changing of security levels or categories of information.

c. Access. Each IS will have an associated access control policy that will include features or procedures to enforce the access control measures required for the information within the AIS. The identity of each authorized user will be established positively before granting access.

d. Controls. The level of control and protection will be commensurate with the maximum sensitivity of the information present in the system and will provide the most restrictive control measures required by the data to be handled. This includes personnel, physical, administrative, and configuration controls.

e. Markings. All media will be marked and protected commensurate with the requirements for the highest security classification level and the most restrictive category of information ever stored on the media until the media is declassified or destroyed under this regulation or until the information is declassified or downgraded under AR 380-5.

f. Data Continuity. The file or data grouping accessibility, maintenance, movement, and disposition will be governed by security clearance, formal access approval, need-to-know, and protective markings as appropriate. All files or data groupings will be labeled to ensure that the security classification or special markings are maintained during storage, processing, and communication transfer.
g. data movement.
(a) An Intranet is a collaboration of data networks under the control of an organization and accessible only by that organization's employees or authorized users.
(b) Examples of differently classified networks are an Unclassified network connected to a Secret network, Secret network connected to TS network, Unclassified network connected to TS network.
(c) Refer to DISC4 for the list of approved firewalls, devices with firewall functions (e.g., routers with filtering mechanisms) and HAG.
(d) Refer to NSA for a list of approved encryption algorithm and device for differently classified data.

g. Contingency Planning. Establishing a disaster recovery capability requires devising recovery procedures and backup for the entire environment (building) and for hardware, software, data, and communication networks. An extremely detailed and broad-scoped disaster recovery plan, Continuity of Operations Plan (COOP), can bring the organization back to a functioning business in the event of almost any type of disaster. A sample checklist (EVAL.DOC) and more detailed instructions on preparing a COOP are found in Appendix C.

(1) The plan should address various levels of response to a number of possible disasters and should provide for partial or complete recovery in the areas of:

(a) The building (environment)

(b) System software and utilities

(c) Application programs

(d) Hardware, remote microcomputers, and terminals

(e) Manual forms, staff assignments and responsibilities during the disaster

(f) Data entry support

(g) On-site and off-site database file storage and retention

(h) System operating procedures locally and at remote user areas

(i) Adequate updating and maintenance of the disaster plan

(j) All communication networks (private leased backbone, LANs, public dial-up, and so
forth)

(k) All related communication hardware

(2) A good data communication network disaster plan should take the following into account:

(f) Action to be taken in case of partial damage, threats such as a bomb threat, fire, water or electrical damage, sabotage, civil disorders, or vendor failures.

(g) Procedure for imposing controls over the network until the system returns to normal.

(h) Storage of the disaster recovery procedures in a safe area where they cannot be destroyed.

h. Security Plans evolve into the accreditation documents and will be maintained to reflect system changes.

i. Accreditation packages will be completed as per the guidance in chapter 3.

(a) The name of the decision-making individual who is in charge of the recovery operation. A second individual should be indicated in case the first manager is unavailable.

(b) Availability and training of backup personnel with sufficient knowledge and experience in data communications.

(c) Recovery procedures for the data communication facilities (WAN, LAN, etc.). This is information on the location of circuits, and who to contact for backup data circuits and documentation.

(d) How to replace damaged data communication hardware and software that are supplied by vendors. Outline the support that can be expected from vendors, along with the name and telephone number of the person to contact.

(e) Location of alternative data communication facilities and equipment, such as connector cables, local loops, common carrier switching facilities, satellite, and public data networks.

j. Risk Management will be completed as per the guidance in chapter 5.

Systems Security Authorization Agreement (SSAA). An SSAA shall be developed and maintained for the life of each IS in accordance with DODI 5200.40.

m. CDAP Process. This process is offered by LIWA for the purpose of providing the SA and the NA with assistance in reviewing security of Army networks and computers. This assistance is provided through a number of programs including the Computer Defense Assistance Program (CDAP). The procedures to identify AIS vulnerabilities are governed by this regulation, and the procedures to verify vulnerabilities are governed by AR 380-53

The CDAP is organized and structured in phases). Each phase provides a layer of evaluation and builds on the preceding

phase/phases. This phased approach, allows the requesting unit commander or activity to customize the program to meet needs and expectations. Phases 1 and 2 provide authorization and information about the target AIS network or subnet and establish the "rules of engagement." Phases 3 and 4 provide identification of suspected AIS vulnerabilities. Phases 5 and 6 provide verification of suspected vulnerabilities and analysis of network protection capabilities. Phase 7 provides technical support to assist in the mitigation of these vulnerabilities. Phase 8 provides a final report to the requesting unit/activity. This report is considered "sensitive" and dissemination of information will be controlled by the requesting unit/activity.

(1) *Phase 1 - Request/Authorization.* The unit commander or activity responsible for the security of the target AIS must make a formal written request to participate in the program and/or provide the ACERT with specific authorization to analyze and penetrate the target network. The primary objectives of phase 1 are: Establish written request/authorization to conduct network security analysis of the target AIS network or subnet. The request will confirm the proper posting of the "notice and consent to monitoring" as specified in AR 380-53, paragraphs 2-4 and 2-5, on all target networks and subnets. Systems without appropriate banners will not be allowed to participate in the CDAP. Establish priority for the effort and enter the request into the CDAP database for control, management, and scheduling. Establish operating/mission parameters for the target network or subnet.

(2) *Phase 2 - Fact Finding.* The purpose of this phase is to obtain information about the design and implementation of the target network or subnet and information about individual machines on the network. The primary objectives of phase 2 are: obtain copies of network diagrams, obtain survey information from a sampling of users, obtain information about each and every machine on the network by name and address, operating system (OS), location, and dial-in capabilities.

(3) *Phase 3 - Network Survey.* The purpose of this phase is to compare the target network layout as designed/implemented by the unit to a layout mapped from the outside. This helps to identify potential back doors into the network and assists with security improvement recommendations. The primary objectives of phase 3 are: Identify all machines on the network at the subnet level, identify all dial-in connections into the network at the machine, compare results with the documentation provided by the unit/activity, identify all paths of entry into each network subnet and flag risk areas.

(4) *Phase 4 - Network Scan.* The purpose of this phase is to assess intrusion susceptibility of the network at the machine level. The primary objective of phase 4 is: Identify all machines on the network which can be targeted for potential compromise/intrusion.

(5) *Phase 5 - Network Penetration.* This phase is authorized under AR 380-53 only and is provided here for reference only. The purpose of network penetration is to examine the degree and depth of information compromise which could be obtained by potential intruders and to assess the ability of the target network/subnet to detect the presence of an intruder. Due to the intrusive nature of this phase, this phase is optional but highly recommended. The primary objectives of phase 5 are: Exploit only vulnerabilities identified during the scanning phase, exploit vulnerabilities to the point of obtaining "superuser" access to the target machine or network.

(6) *Phase 6 - Penetration Verification.* This phase is authorized under AR 380-53 only and is provided here for reference only. The purpose of penetration verification is to provide positive verification to the requesting unit or activity that system level compromise had been obtained and assess network intrusion detection. Due to the intrusive nature of this phase, this phase is optional. The primary objectives of phase 6 is to provide positive verification of system

or machine compromise in the form of a message or new user account.

(7) *Phase 7 - Technical Support.* The purpose of the technical support phase is to provide support to the requesting unit or activity to fix the vulnerabilities identified during the vulnerability analysis and penetration phases. The primary objective of phase 7 is to assist the requesting unit or activity with security or configuration fixes needed to correct the vulnerabilities found during the vulnerability analysis and penetration phases.

CHAPTER 2, SECTION II, III, & IV: SOFTWARE, HARDWARE, AND PHYSICAL SECURITY (DEV BY COMMITTEE # 2)

SECTION II
Software Security

2-5. Software control is achieved by establishing the following procedures:

a. The IAPM appoints a qualified and responsible person for software accountability (i.e. IAM, IASO, or SA) (Paragraph 2-5a, AR 25-IA). The appointed person will:

(1) Develop Standard Operating Procedures (SOP) on who is authorized to load approved software. (Paragraph 2-5b, AR 25-IA).

(2) Develop a Software Management control process (manual or automated) that identifies all software loaded on AIS. (Paragraph 2-5d, AR 25-IA) The control process will include the following information as a minimum:

- ??Title/description
- ??Vendor
- ??Version
- ??Licenses Agreement
- ??Platform (type of equipment software operates on; i.e. PC, mainframe, server)
- ??POC or SA

b. The IASO conducts a software risk analysis. If the risk analysis reveals unacceptable risk from attacks by malicious software, additional measures (i.e., commercial “anti-virus” programs, tamper-resistant holographic seals, non-technical security methods, etc.) will be employed to reduce this risk to an acceptable level.

(8) *Phase 8 - Final Report.* An executive summary report will be provided to the requesting unit or activity outlining impacts and recommendations for securing the target network or subnets. The full report will provide detailed information on impacts, risk assessments, and recommended fixes to secure the target network or subnet. This report will be considered "security sensitive" and will be released to the requesting unit or activity only

c. Upon acceptance for operational use, whether developmental, governmental off the shelf (GOTS) or commercial off the shelf (COTS), the SA/IANM/IASO must keep the software under close and continuous configuration management controls. These controls identify and prevent unauthorized changes and lessen the risk of introducing untested and malicious software. Figure 2-1 illustrates the software control process. A master (original) copy of the software must be safeguarded against misuse, damage, theft, and/or alteration. Production copies of software, when feasible, should be generated from the master or original copy, as required, for actual production operations. Physically secure software media, documentation and program specifications within an area approved for storage at the appropriate classification or sensitivity level. System and application software will be protected and backup copy maintained. (Paragraph 2-5e, AR 25-IA)

d. Documentation that addresses software design and capabilities will be maintained for the use of programming, operations, and user personnel. Only personnel performing official duties should

be allowed access to this software documentation.

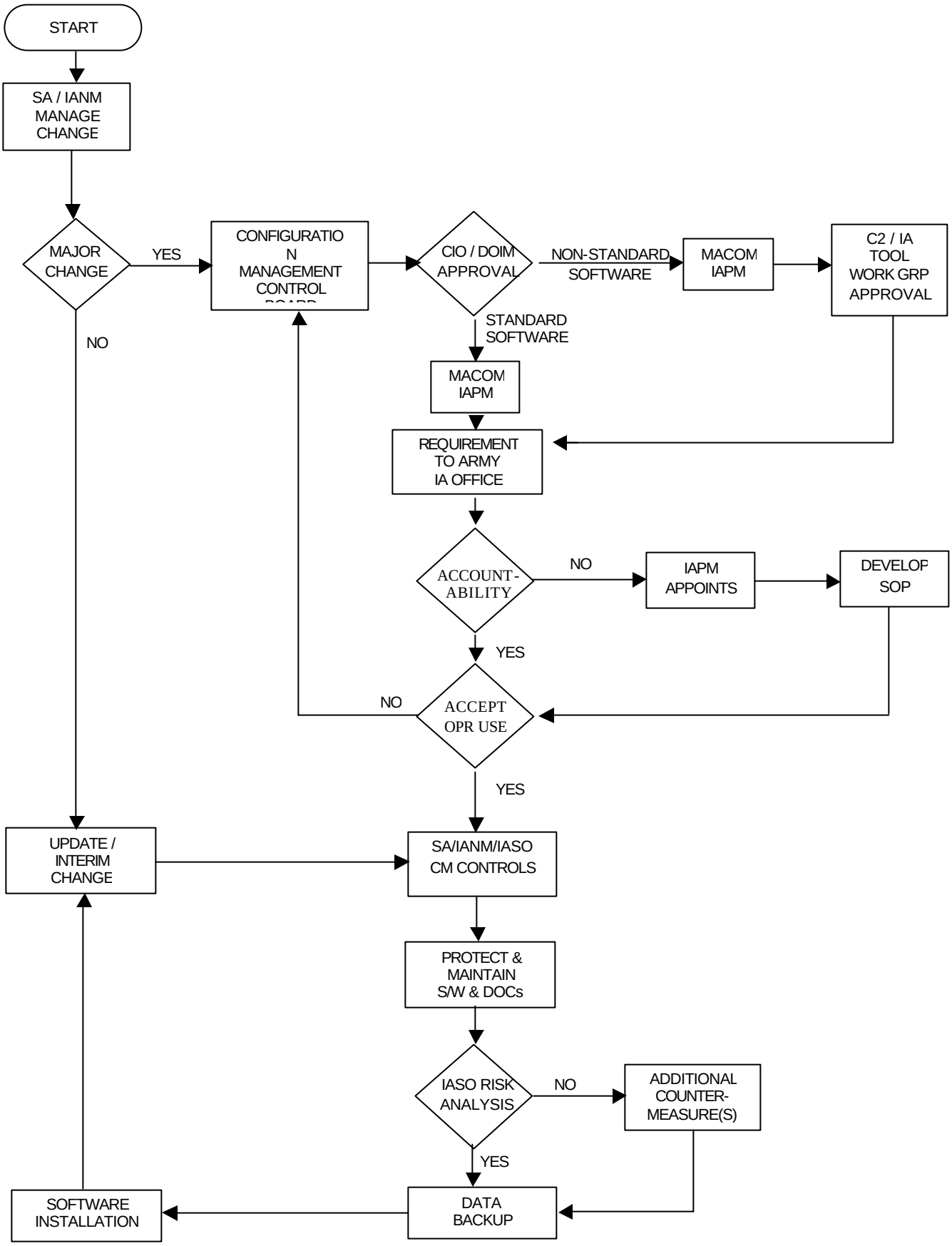


Figure 2-1 Software Control Process

e. Manage Software changes (Paragraph 2-5f-h, AR 25-IA)

(1) The SA/IANM documents, installs, and monitors changes to AISs. Changes to system software fall within one of three categories:

(a) Major Change. A major modification or new capability to software programs. The Configuration Management Control Board (CMCB) reviews all requirements and discrepancies.

(b) Update Change. A deficiency, discrepancy, or problem that typically requires a minor correction to documentation or software to comply with existing requirements.

(c) Interim Change. A temporary change or fix (i.e., patches, service packs, etc.) to software that is required to continue operations.

(2) Perform data file backups to protect data integrity, which may be damaged during any system change. Although a simple procedure, this is one of the cornerstones of software and data security that is often overlooked.

f. Receive approval from DOIM or equivalent official for purchase or use of any software before installing on AIS. List(s) of approved or standardized software can be obtained from IAM. (Paragraph 2-5d/g, AR 25-IA)

g. Submit requests for non-standard Army applications software and programs thru MACOM IAPM to the C2/IA Tool Working Group for approval prior to being integrated and used by any Army element. (Paragraph 2-5c, AR 25-IA)

h. Submit requests for software to CECOM CSLA through MACOM for review of IA Blanket Purchase Agreement (BPA).

2-6. Protection of Data-base management systems

a. The DOIM or equivalent official appoints a responsible person as Data-base Administrator for data-bases and assigns appropriate duties. (Paragraph 2-6c, AR 25-IA)

b. Protecting shared data-bases is essential, as they represent a significant asset and frequently reveal considerably more information taken as a whole than can be obtained from their individual parts. Commercial data-base management systems have different characteristics, such as those listed below, that affect their security stability and must be considered when acquiring a system for handling classified or unclassified information: (Paragraph 2-6a, AR 25-IA)

(1) Distributed data-base access and synchronization

(2) Data-base integrity

(3) Data-base availability (fail-over, recovery, and restart functions)

(4) Data and program protection mechanisms that control read and write permissions.

(5) Audit mechanism and utilities

c. When data base management systems containing classified defense information are used, the classified identifiable element (i.e. word, field, or record) within the data base must be protected according to the highest security classification of any data-base element. If the data-base cannot provide field protection, then it should provide record protection to the highest security classification level of the fields within the record. Data-base systems that do not provide protection at the record or field level will be restricted to operation in the dedicated or system high security mode. In all cases the data-base management systems (DBMS) must meet the minimum trust requirements.

d. Data-base systems that bypass the production of operating system audit trail data must produce their own audit trail data similar to those prescribed for the operating system. These audit trails must also be used in determining the confidentiality, integrity, and availability of the automated system and the data contained therein.

e. Designers and developers of data base management systems, in coordination with security specialists and proponents for the data elements, must consider the effect that compilation of data will have on the final security classification of the data-base system. The degree to which a given user can be reliably denied access to portions of the data-base will influence the final classification decision. The DBA implements controls of the data-base schema to prevent unauthorized modifications of the database system (AR 25-IA, paragraph 2-6d)

f. Figure 2-2 illustrates the Data Base Management Protection Process.

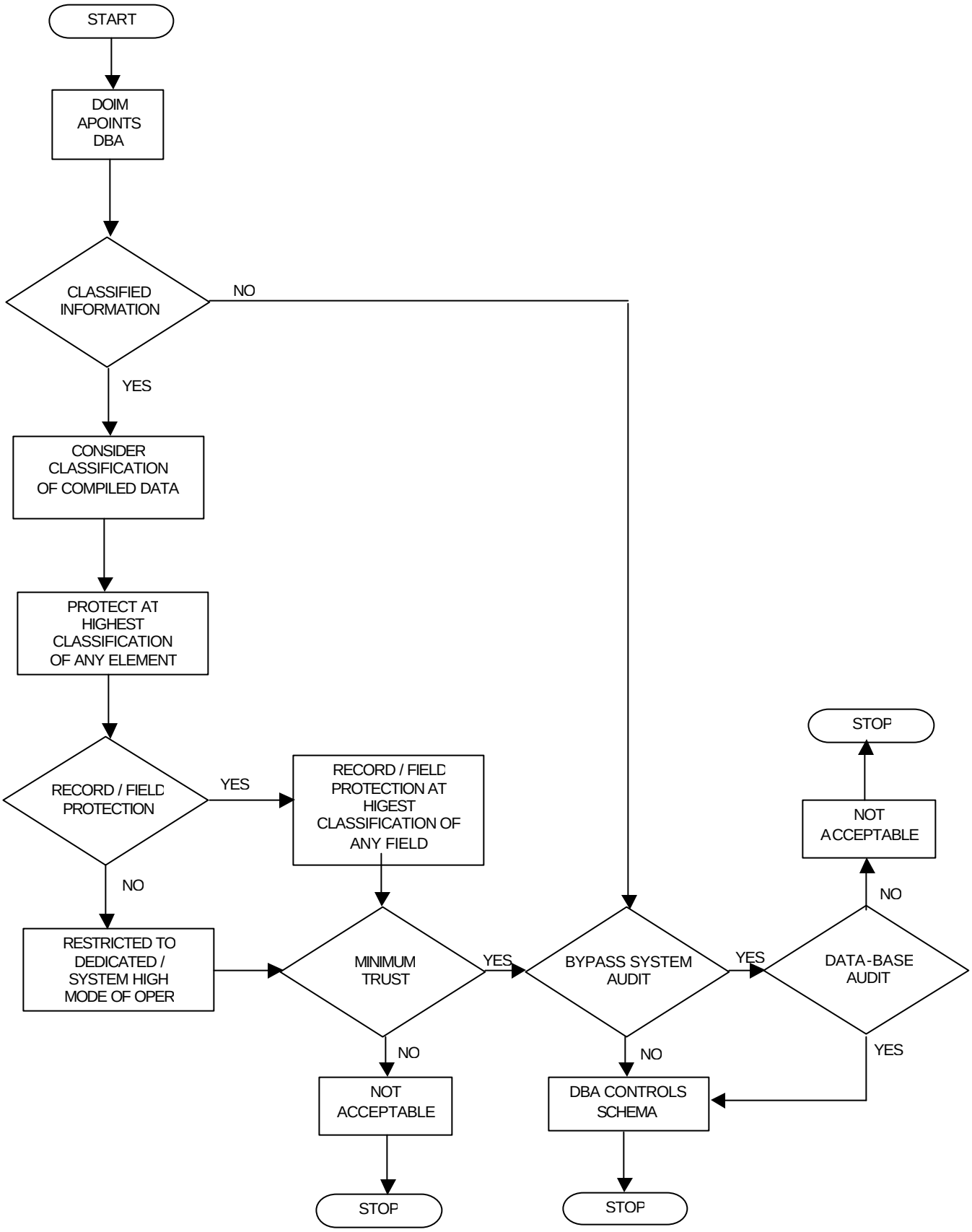


Figure 2-2 Data-base Management

2-7. Software security packages

a. To protect classified information, ensure software security packages are evaluated by the NSA and are included on the IA Products and Services Catalogue. (Paragraph 2-7a, AR 25-IA)

b. To protect unclassified information, ensure software security packages are evaluated by the National Institutes of Standards and Technology (NIST). (Paragraph 2-7b, AR 25-IA) and are included on the NIST Products and Services List. Products other than those evaluated by the NIST may be used; however, such products must be approved by the DAA and based on a valid justification.

c. The decision to use software security packages will be based upon:
(1) Cost
(2) Evaluation Assurance Levels (Paragraph 2-7c, AR 25-IA)
(3) Performance evaluation
(4) Risk Assessment advantages and disadvantages (Paragraph 2-7c, AR 25-IA)
(5) Site licenses
(6) Maintenance
(7) Source of software

d. If the purchase or annual lease costs of products not listed in the NSA IA Products and Services Catalogue exceeds $50,000.00, the request must be submitted to HQDA (SAIS-IAS) for approval. (Paragraph 2-7d, AR 25-IA)

2-8. Software design and test

a. Software security requirements must be considered in the future design, development, and acquisition of Army systems.

b. Examination of the control over the procedures used to develop computer programs is an integral part of the software certification and AIS accreditation process. The key to eventual certification is to develop systems that are easily understood and verifiable.

c. Programs must be completely tested by the Certification Authority (CA) before becoming operational. Both valid and invalid data must be used for testing. Testing is not complete until all security mechanisms have been examined and expected results are obtained and attempts to circumvent or defeat these mechanisms fail.

d. Upon completion of the maintenance or modification of software, independent testing and verification by the CA will be required before returning software to operation.

e. In accordance with life cycle management milestones, the CA will develop a Test and Evaluation Master Plan that includes current, validated threats to each information system.

f. The CA must certify all information processing elements prior to use on an operational, accredited system. These elements include functions, utilities, applications software, operating system software, communications software, program files (.COM), binary files (.BIN), and any executable code (.EXE, JAVA, etc.) or other automated processes. System configuration/information files (.CFG, .SYS, .DLL, etc.), batch files (.BAT), text/data files (.DAT, .TXT, .RTF, .HTM, etc.) graphic files (.BMP, .JPG, .GIF, etc.) word processing documents (.WP, .DOC, .etc) and spread sheets (.XLS, etc.) do not normally require certification. However, these files may have executable code in the form of functions or macros that must be identified and considered before installing on an accredited system.

g. System software can originate from numerous sources. This includes government agencies, commercial vendors, independent software developers, and

unknown sources. The latter two cases cause the most concern. The risk that malicious logic is embedded in the software code or the software may allow existing security features to be bypassed, is much greater. Generally, software originating from government sources or corporate giants, represents a lesser risk than independently developed software or software originating from questionable sources, (e.g., internet websites, buddies, etc.). Malicious logic in the form of Trojan horses, logic bombs, viruses, etc., may be embedded in the software code that allows an unauthorized user access to the system or may modify or destroy systems files.

h. The CA must certify software that implements security features (e.g., identification and authentication, audit, object reuse, discretionary or mandatory access controls, labeling, etc.). Security features must be tested and evaluated to ensure DOD and DA policies are implemented.

i. Where a requirement exists for which no evaluated or assessed product exists the organization may request that DA perform an assessment. Send requests to HQDA (SAIS-IAS). If the product does not have Army wide applicability the request may be denied. The assessment may take a considerable time to complete – possibly up to a year.

j. The CA at the requiring organization may have no choice but to assess the product. The CA must select a suitable product, then test and certify it for use on the accredited system. To accurately validate the implementation of the security features, the CA must have considerable technical skills, knowledge of the software and functionality of the security features.

k. Figure 2-3 illustrates the software certification process. If the software does not implement a required security feature, install the software and test existing system countermeasures to ensure they still work as required. Ensure the software cannot be used to bypass any system security feature. If any of the tests fail, develop a recommendation for DAA approval. If the DAA determines that the risk is unacceptable, additional countermeasures may be needed or use of the software may be denied.

l. If the software has been evaluated or assessed, attain a copy of the report. Test to ensure the security features are not interfered with and document this testing. Perform a risk analysis, develop a new accreditation recommendation, and have the DAA make a new accreditation recommendation. If the DAA determines that the risk is unacceptable, additional countermeasures may be needed or the software may be denied.

m. If the software has not been evaluated or assessed, update the Security Test & Evaluation (ST&E) plan to include the testing of the security features implemented by the software. The objective is to ensure the security feature is implemented according to guidance. Also, test existing software countermeasures to ensure that they still work as required once the software is installed. Then, run the new software and determine if any of the security features can be bypassed while using the new software. Document the results. Perform a risk analysis, develop a new accreditation recommendation, and have the DAA make a new accreditation recommendation. If the DAA determines that the risk is unacceptable, additional countermeasures may be needed or the software may be denied.

n. Correlate all T&E events or results with the Army Vulnerability Database. (HQDA SAIS)

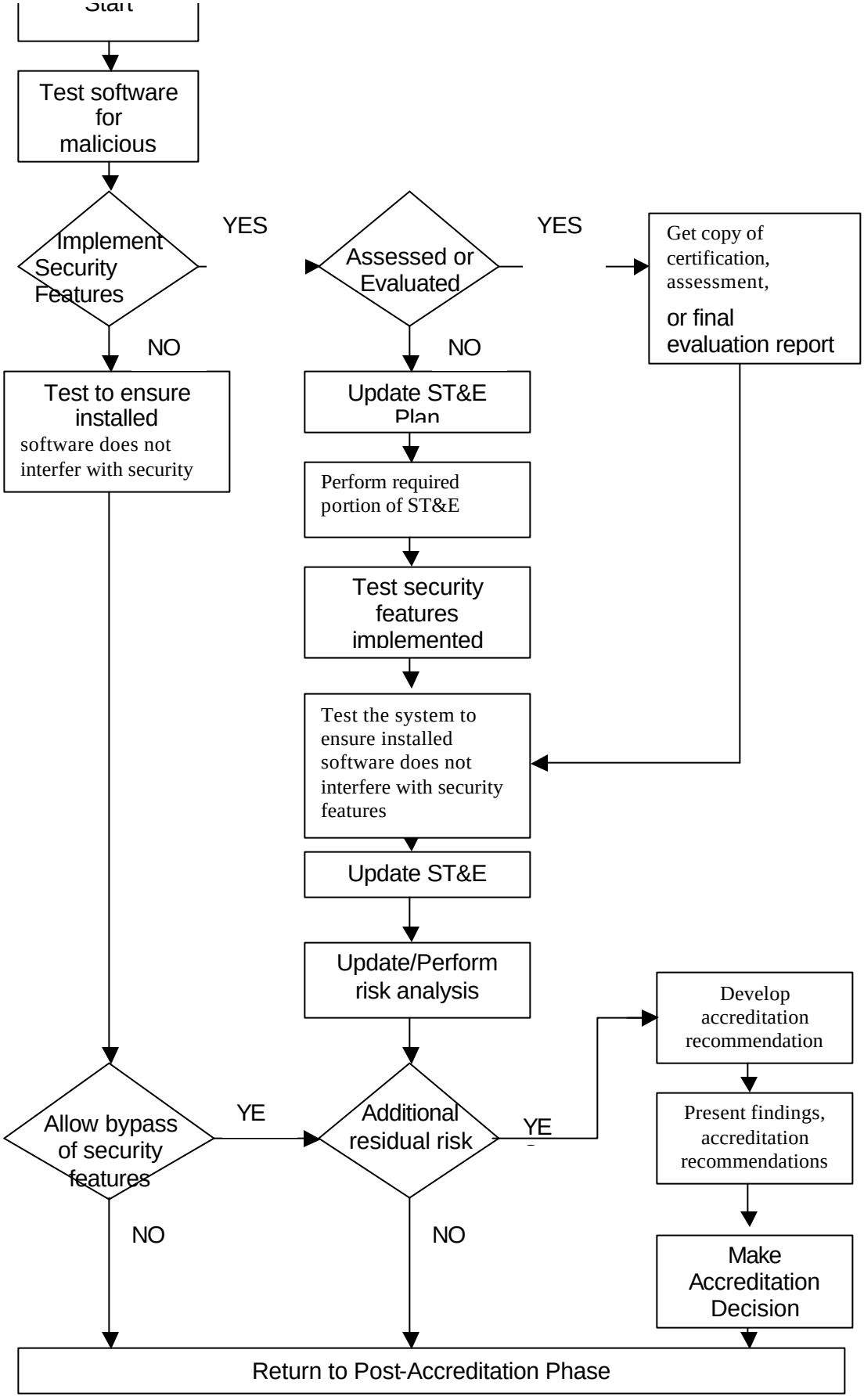


Figure 2-3 Software Design and Test

SECTION III
HARDWARE SECURITY

2-9. Hardware-based security controls.

a. Hardware-based security controls represent an important factor when evaluating the security environment of any Army system. The absence of hardware-embedded security features or the presence of known hardware vulnerabilities will require compensation in other elements of the security program. The following issues are to be considered during this process:

(1) Accountability: Primary hardware security begins with property book accountability. The Hand Receipt holder, SA, IANM, and IAM should always be involved when equipment is moved, received, transferred, or transported. (2-9a/d)

(2) Review requirements document: A thorough understanding of system, functional, and operational requirements will aid in the development of the security policy. The CA must review documentation describing how and where the system will be used. The purpose of this review is to identify and comprehend the security requirements. Some examples of requirement documents that may contain security requirements are Statement of Work (SOW), Concept of Operations (CONOPS), Support Level Agreements (SLA), Program Management Directive (PMD), Mission Need Statement (MNS), and Operational Requirements Document (ORD).

(3) Determine environmental requirements:

(a) Environmental requirements (e.g., physical mobility, tactical conditions, temperature, humidity, sand/soil, location structure, etc.) identify the need for additional security measures. These conditions must be identified and clearly understood.

(b) Certifying and accrediting mobile or deployable hardware is more complex because it must address all possible area of responsibility (AOR), operating environments, as well as the various hardware configurations (i.e., in garrison, storage, transit, and deployed). Since it is difficult to certify and accredit a mobile system at all possible locations, the DAA may accredit the system for a generic environment. That is the baseline environment, which describes the minimum protection required for each state of operation. Conditions at the actual deployed site may dictate the need for site ST&E and an informal risk analysis to determine unique or additional protection required. Any significant change to the mobility requirements, specified environments, or hardware architectures may require the system to be re-certified and re-accredited.

(c) Although not mandatory, the CA may want to consider some specific environmental operational requirements when performing Certification and Accreditation. The operational requirements could include power, air conditioning, ventilation and heating systems. Use system criticality to help determine the need for inclusion of these requirements.

(4) Determine Hardware Criticality:

(a) Criticality is a measure of the importance of the hardware (including the data it processes) and the length of time it is out of operation before its loss results in an adverse impact on mobilization, deployment, or national emergency. The level of criticality is dependent on the organization's ability to support mobilization, deployment, or national emergency operations without the system. The criticality of hardware is independent of the sensitivity level of the information processed. Criticality is documented in the system security policy. Use the following to identify hardware criticality:

?? Mission Critical: The loss of the hardware would cause immediate stoppage

of direct mission support of mobilization, deployment, or national emergency.

?? Mission Essential: The loss of the hardware would cause an eventual stoppage of direct mission support of mobilization, deployment, or national emergency.

?? Mission Impaired: The loss of the hardware would have an effect on (but would not stop) direct mission support of mobilization, deployment, or national emergency.

?? Non-mission Essential: The loss of the hardware would have no effect on direct mission support of mobilization, deployment, or national emergency.

b. Multiple layers of security are normally involved in any secure environment or security plan. No one solution will address all possible scenarios. The following factors are to be considered when protecting hardware/firmware from compromise, unauthorized use/access, or manipulation: (2-9a)

(1) Personnel access controls
(2) Physical access controls
(3) System/network configuration
(4) Threat
(5) System access controls (passwords, etc.)
(6) Physical surroundings (building, tent, vehicle, etc.)
(7) Classification of equipment/information

c. Submit requests for hardware/firmware approval through DAA, Material developer, CIO, and or IM Manager prior to being integrated into AIS. (Para 2-9b/c, AR 25-IA)

d. Upon acceptance for operational use, whether developmental, governmental off the shelf (GOTS) or commercial off the shelf (COTS), hardware must be kept under close and continuous configuration management controls so that unauthorized changes are not made. Hardware/firmware must be safeguarded against misuse, damage, theft, and/or alteration. Physically secure hardware, documentation and specifications at appropriate location/level. The Configuration Management Control Board will determine the necessity for backup hardware. Strict configuration management controls will be enforced to lessen the risk of introducing untested and malicious firmware. (Para 2-9e, AR 25-IA)

e. Version changes are submitted to the IAPM for configuration control/oversight IAW paragraph 2-9f, AR 25-IA.

f. The Special Security Officer approves the release of hardware/firmware from Sensitive Compartmented Information Facilities (SCIF), in coordination with the IAM. The following factors should be considered when developing procedures:
(1) SCIF points of egress that would allow removal
(2) Measures in place at those points (guards, door locks, alarmed exits, etc.)
(3) Personnel in positions most likely to be aware of removal

g. Submit requests for hardware/firmware acquisition requirements to HQDA-SAIS-IAS. (Para 2-9h, AR 25-IA)

h. Submit requests for hardware/firmware to CECOM CSLA through MACOM for review of IA Blanket Purchase Agreement (BPA).

i. Figure 2-4 illustrates the hardware control process.

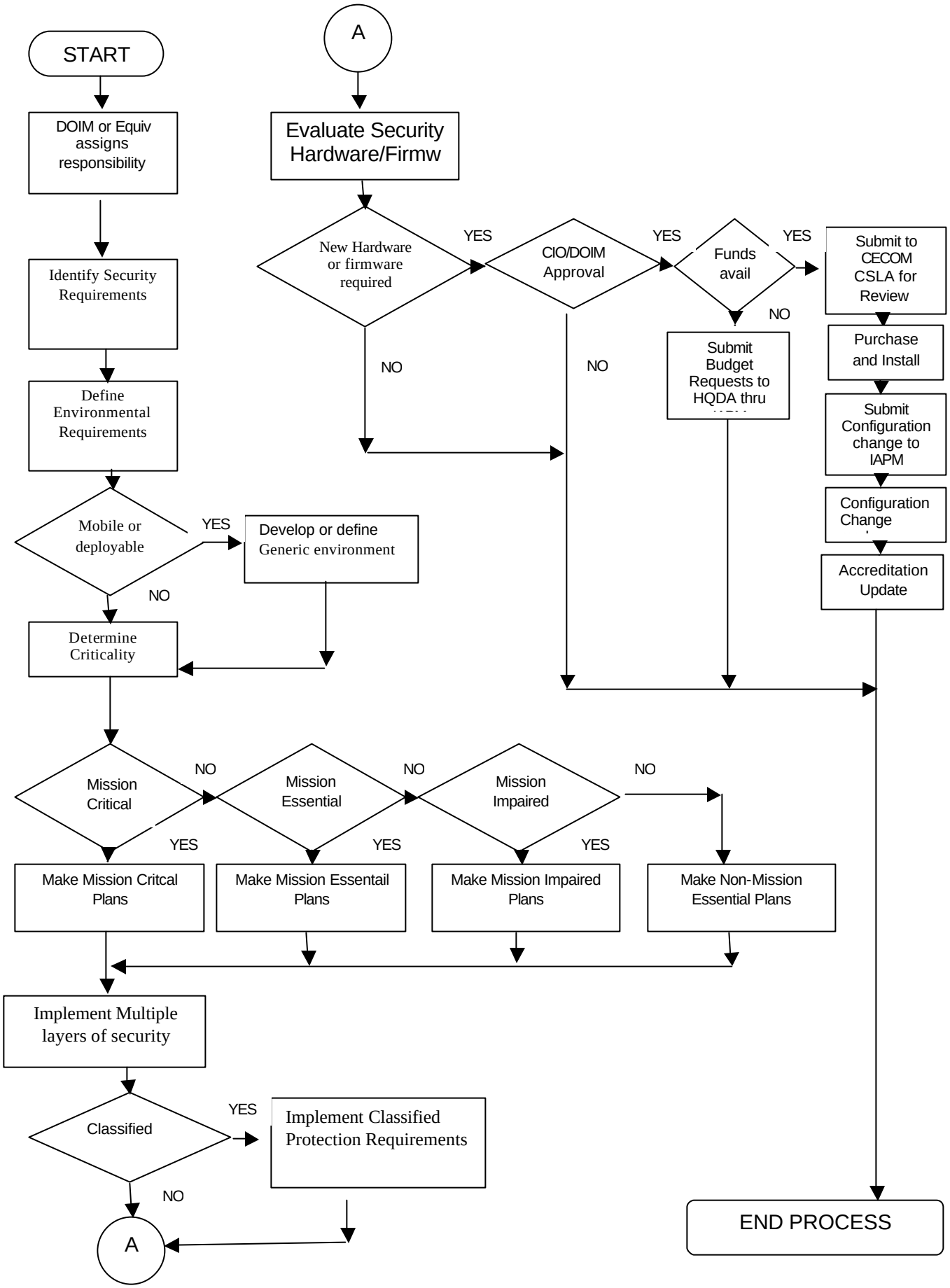


Figure 2-4 Hardware Security

2-10. Maintenance Personnel

a. Security investigations/clearances at the appropriate level should be on file or obtained for maintenance personnel that service classified systems.

b. Cleared personnel who perform maintenance or diagnostics do not normally require an escort. Need-to-know for access to classified information must be enforced. A cleared and technically knowledgeable individual must always escort uncleared maintenance personnel.

c. Maintenance personnel who do not access classified data during their maintenance operation should, nevertheless, be cleared for the highest level of data processed on the system. However, if this is not feasible, maintenance personnel will be monitored at all times during their maintenance operation by individuals with the technical expertise to detect unauthorized modifications.

d. Ensure non-U.S. citizens do not perform maintenance on TS, SCI, SIOP–ESI, and SAP AIS.

e. When non-U.S. citizens are employed to maintain other than TS, SCI, SIOP–ESI, and SAP AIS, such use will be addressed as system vulnerability in the risk assessment and appropriate countermeasures will be employed.

SECTION IV
PHYSICAL SECURITY

2-11 Security Objectives and Safeguards

a. A balanced AIS security program must include a firm physical security foundation with the following objectives:
(1) Safeguard personnel.
(2) Prevent unauthorized access to equipment, facilities, material, media, and documents.
(3 Safeguard against espionage, sabotage, damage, and theft.
(4) Reduce the exposure to threats that could cause a denial of service or unauthorized alteration of data.
(5) Create and promote physical security awareness.
(6) Coordinate installation operations security (OPSEC), crime prevention, and physical security programs to protect against the total threat.

b. Facilities that house systems, computer rooms, network components (for example, routers or file servers), and related sensitive areas may be designated as restricted areas or mission essential vulnerable areas under AR 190–13. Facilities and systems so designated will be included in the installation physical security plan required by the same regulation. Periodic physical security inspection requirements are also contained in AR 190–13 and AR 190–51.

c. Facilities that house systems processing SCI material will be subject to the provisions in DCID 1/21.

d. Particular attention must be paid to the physical security of AIS that are not operated or otherwise attended continuously. An AIS that processes classified defense information must be properly declassified prior to being left unattended, unless it is secured in areas or containers approved for storage of classified material under AR 380–5.

e. The number and diversity of Army AIS (fixed and deployable systems) and installations make it impractical to establish universal, rigid physical security standards. However, adequate physical security at each installation is essential to achieving a secure data processing environment. Physical security standards must be based on an analysis of both wartime and

peacetime mission criticality, sensitivity levels of the information processed, overall value of the information to the mission of the organization, the local criminal and intelligence threat, and the value of the automated equipment.

f. Physical security will be provided through an in-depth application of barriers and procedures, which may include continuous monitoring (human or electronic) of the protected area. Barriers and procedures include structural standards, key control, lighting, lock application, access control devices, containers, badges, guards, inventory and accountability, or other supplementary controls.

g. Physical access controls commensurate with the level of processing will be established to deter unauthorized entry into the facility and other critical areas (such as input or output, programming, data preparation, and storage area) that support or affect the overall operation.

j. Facilities housing AIS equipment will be of sufficient structural integrity to provide effective physical security at a reasonable cost. Trained physical security specialists will be consulted in all phases of selection, design, and modification of such facilities to provide expertise in physical security requirements.

2-12 Physical Security for Small Computers

a. Many AIS, including some file servers, clearly do not warrant the physical protection detailed in paragraphs above. These include personal computers, workstations, notebook computers, and laptop computers, as well as other AIS where the computing environment is fully integrated into the work environment. Application of the above standards will depend on AIS size, complexity, manufacturer specifications, number of terminals, sensitivity of data, and environmental requirements. If the mainframe physical security requirements do not apply, the provisions in this paragraph will be followed.

b. Physical security requirements must be considered and selected based on the sensitivity and classification of data being protected, as well as assessed risk to the information and the risk of equipment theft. The physical security requirements must be examined to ensure protection of equipment is cost effective, that the impact on objectives is negligible, and that the level of risk is acceptable to the local Commander.

c. All AIS must be protected, and physical security requirements must be carefully selected.

(1) An AIS with non-removable media that processes classified information must be stored in an area or a container approved for safeguarding classified media per AR 380–5.

(2) An AIS with SBU in formation on non-removable media should be in a locked office or building during non-duty hours or be otherwise secured to prevent loss or damage.

(3) When users leave their workstations or personal computers, they will log-off or lock the keyboard or screen until re-authentication.

(4) Workstations and personal computers should include a local “idle lockout/screen saver” feature that automatically locks an unattended screen requiring re-authentication before unlocking the system (for example, a password protected screen saver). A local risk assessment will be completed to determine the minimum time the idle lockout/screen saver feature will activate.

d. A checklist is provided at Figure 2-5 to assist in identifying physical security issues.

PHYSICAL SECURITY CHECKLIST

ITEM	YES	NO
1. Does the physical security plan address the following:		
a. Personnel		
b. Access to		
(1) Equipment		
(2) Facilities		
(3) Media		
(4) Documentation		
(5) Materials		
c. Espionage		
d. Sabotage		
e. Damage		
f. Theft		
g. Physical Security awareness training		
h. Logon/logout procedures		
2. Are facilities that house computers or other major automatic data processing Equipment in a restricted area?		
3. Does plan account for differences in physical security requirements due to different operating environments caused by wartime versus peacetime activities?		
4. Physical security for small computers in open office environments accounted for?		
5. Classified areas managed in accordance with DCID 1/21 requirements?		
Figure 2-5		

CHAPTER 2, SECTION V, VI, & VII:
PROCEDURAL, PERSONNEL SECURITY, AND INFORMATION SYSTEMS MEDIA (DEVELOPED BY COMMITTEE # 3)

2-13 Accountability. The responsibility for the success of an organization lies with it's senior commanders or directors. They They establish the organziations information assurance program and it's overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately the head of the organization is responsible to ensure adequate resources are applied to the program and that it is successful.

a. The IAM is the focal point for IA programs within each organization. The IAM is responsible to the organizational commander for the overall IS security program. The IAM executes the security program on behalf of the MACOM IAPM executing the organizations day-to-day management of its IA program. The IAO/IANO and other IA security officials will work with the IAM to establish a viable IA security posture. The IAM is responsible for coordinating all security-related interactions among elements involved in the organizations IA and site security program – as well as those external to the organization.

b. IA personnel should be positioned within an organization to ensure a proper balance between operational concerns as well as network operations.

c. Effective administration of users' computer access is essential to maintaining system security. User account management focuses on user account authorization. User account authorization will focus on identification, authorization, and access. To ensure users are aware of their accountability requirements refer to paragraph 2-2b.

d. Procedural security measures should produce a higher corresponding level of security at a minimum financial expenditure.

2-14 Classified Processing.

a. Processing, handling and storing classified data.

(1) For additional specific guidance, refer to DOD 5200.1-R and AR 380-5. For specific guidance for processing, storing and handling SCI, refer to DIAM 50-4 or AR 380-28.

(2) Classified processing will only be conducted on systems accredited to process classified information.

(3) Facilities that house systems, computer rooms, networks components and related sensitive areas may be designated as restricted areas or mission essential vulnerable areas under AR 190-13.

(4) Facilities that house systems processing SCI material will be subject to the provisions in DCID 1/21. All IS equipment used for processing handling and storing SCI will be operated and secured in compliance with Defense Intelligence Agency Manual (DIAM) 50-4, Joint DODIIS, DCID 1/16, this regulation and/or successor documents.

(5) An IS that processes classified defense information must be properly declassified prior to being left unattended, unless it is secured in areas or containers approved for storage of classified material under AR 380-5.

(6) Physical access controls commensurate with the level of processing will be established to deter unauthorized entry into the facility and other critical areas that support or affect the overall operation.

(7) An IS with non-removable media that processes classified information must be stored in an area or a container approved for safeguarding classified media per AR 380-5.

(8) When users leave their workstations or personal computers that processes classified information in an open storage area, they will log-off or lock the keyboard and screen until re-authentication.

(9) An IS authorized to process classified information must be marked with the highest level it is accredited to process. Mark the

system and all media with SF 706, 707, 708 or 712 as appropriate.

b. Declassifying and releasing media. Refer to Section VII of this PAM.

2-15 Password Control.

a. User identification (user-ID) and passwords, because of their cost-effeciency and ease of implementation, are the most common identification and authentication (I&A) procedures. Because of their vulnerablitlity to interception or inadvertent disclosure, they are also the weakest of I&A methods. Passwords are only effective when used properly. Inappropriate passwords create some of today's most common information system vulnerabilities.

b. IASO or designated representatives are responsible for establishing and maintaining the I&A management program for the system, creating, distributing, controlling, and deleting indentifiers and passwords, and maintaining the criteria outlined in this PAM. Should mission requirements dictate, system administrators can be assigned to assist IASOs in I&A management.

c. Prior to issuing passwords and user-IDs, make sure the user has taken appropriate computer security training. Make sure the user is briefed on the importance of protecting their user-ID and password; reporting any suspicious activity, fraud, waste, and abuse; and the use of system monitoring following the incident reporting process found in this DA PAM..

d. The organizations IASO will ensure a method is in place to authenicate requests for information system access, i.e., valid user background investigation, clearance, and need to know, as appropriate, before issuing passwords.

e. Use passwords generated by the IS if the system has that capability.

f. Passwords generated by the user must meet the criteria of AR 25-IA. Passwords will be at least eight alphanumeric characters (upper and lower case) with at least two numeric/special characters (1, 2. @.#.$.%. etc). Never make a password related to one's own personal identity, history, or environment.

g. Generic password assignment is prohibitied (e.g., a system having "welcome" as the password for all newly created accounts) unless the user is required to change the password upon initial assignment.

i. Limit the number of attempts allowed for correct password entry. Set the degree of password entry protection and the number of allowed entry attempts according to the sensitivity of the protected data. Normally three attempts are permitted.

j. When the maximum amount of password attempts are exceeded, lock out the user-ID and/or terminal from use. Make sure these procedures cannot be defeated by a user, or used to cause a denial of service by locking out all user-IDs or terminals. Make sure procedures are in place so the user must request reinstatement from the IASO/system administrator.

k. Keep user-IDs unique and assign them to only one person. Do not reissue the user-ID to another person for 1 year after its previous deletion.

l. Each user is responsible and accountable for their own password.

m. Users must memorize their password. Do not place passwords on desks, walls, and sides of terminals or store them in a function key, log-in script, or the communications software. If documentation is necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a safe.

n. Users must enter their identifier and password upon initial access to an information system. A user must enter a password in such a manner that the password is not revealed to anyone observing the entry process.

o. Do not share passwords for individual accounts. Passwords for group and organizational accounts may be shared when necessary for mission accomplishment. When password sharing is

necessary for mission accomplishment make sure the password is changed immediately after shared access is no longer required. If an individual having access to the shared password no longer requires access, the password will be changed immediately.

p. All passwords must be protected based on the sensitivity of the information or critical operations they protect (i.e., a password used to gain access to a SECRET networks is itself classified SECRET). At a minimum, you must safeguard all passwords as "For Official Use Only". User-IDs are an unclassified reference to a user that can be displayed on printouts and in audit trails without compromising the password.

q. Protect passwords during transmission at the same level required for the system or data that the password is protecting. Passwords are typically sent for authentication from a terminal to the system by a communications line. Unless the line is physically protected or encrypted, the password is vulnerable to disclosure by wiretapping and/or sniffers. Prevent this vulnerability by electronic protection or password encryption. Increasing the password length and changing it more often can mitigate this vulnerability.

r. Users may use an established procedure to change their own password whether it is machine or user generated. The user must enter the old password and authenticate as part of the password change procedure.

(1) If the user forgets the password, the system administrator must authenticate the user's identity before changing the password.

(2) If given a generic password (e.g. "password"), the system must prompt the user to immediately change to a new password. If the system is incapable of such a function, the IASO or system administrator must walk the user through the password change procedure.

s. Delete all unnecessary accounts and change all passwords included in a newly acquired system (software or hardware) before allowing any user access to the system.

t. Remove user-IDs and passwords from an IS whenever the user is permanently transferred to another location or terminates employment.

u. Enable or configure the following information system features, if technically possible:

(1) Configure the system to prevent rapid retries when entering a password incorrectly by allowing several seconds to elapse before requesting another password. This delay deters any automated, high speed, trial-and-error attack on the password system.

(2) Following a successful log-in procedure, inform the user of the last successful access to the account and of any unsuccessful intervening access attempts. This aids in uncovering any unauthorized or attempted accesses that may have occurred.

v. To the fullest extent possible, system administrators should use security tools such as "Crack" to provide the best defense against poor passwords.

w. Suggestions for choosing a good password:

(1) Your password is the key to your account. It should be easy to remember, but very hard for someone else to guess.

(2) Do not use your user-ID, a name, a hobby, or a single dictionary word.

(3) Do not use your social security, telephone, or license plate numbers.

(4) Do use a mix of uppercase and lowercase letters and a special character, swim!3MileS, IgolFer*, 2FORU&me.

(5) Do misspell words or replace syllables with numbers and special characters 1onderFul!, For2natE#, aPHORDit$, 56sheVY+, bOOik4u<.

(6) Do use 2 or 3 words together Ear2Knee+, 1BignosE%, BAG4golf!, MaiL4You=.

(7) Do use the first letter of each word in a sentence – "My three dear Daughters are very beautiful!" would become M3dDavb!

And “My one son is a diligent worker!” would become M1siadw!

CHAPTER 2, SECTION VI:

2-16 Personnel Security Standards.

a. All civilian, military and contractor personnel requiring access to an IS meet the requirements of an ADP I, II, or III position (see Appendix K, AR 380-67). Assignment to an ADP position requires a successfully completed security investigation as listed below:

(1) ADP-I. Single Scope Background Investigation (SSBI).

(2) ADP-II. National Agency Check with Local Agency and Credit check (NACLC), National Agency Check with Inquiries (NACI).

(3) ADP-III. National Agency Check (NAC), Entrance National Agency Check (ENTNAC), National Agency Check with Written Inquiries (NACI) or Trustworthy National Agency Check (TNAC).

b. Investigations will be completed prior to appointment to ADP duties or a waiver for appointment will be processed. Procedures for waivers will be processed IAW local waiver to hire/interim security clearance procedures (see Chapter 3, AR 380-67 for guidance). In all cases, the investigative paperwork (SF 86/85 or EPSQ) will be favorably reviewed by security personnel and initiated prior to assignment of duties.

c. Investigation requirements will be documented in all contracts requiring access to an IS. The supporting government personnel security office will process the investigation (TNAC/SF 85P) for contractors not requiring access to classified information.

d. Civilian positions will be designated as Critical Sensitive for ADP-I, Non-Critical Sensitive for ADP-II, and Non-Sensitive for ADP-lll.

e. Criteria for occupying an ADP I, II, or III position are contained in AR 380-67. Commanders or supervisors who become aware of adverse information, either through the formal security investigation or through other official sources, will follow the procedures in Chapter 8 of AR 380-67, which may include suspension from duties.

2-17 Foreign Nationals.

a. Limited Access Authorization (LAA) Employees.

(1) Foreign nationals will not be employed in an IS position which will afford access to classified defense information except when the foreign national meets the provisions for an LAA provided the foreign national’s skill or technical expertise are essential to the national security and are not available from U.S. personnel. LAAs will always be kept to a minimum, consistent with mission requirements, and will be terminated when no longer required.

(2) Commanders may grant individuals with an LAA, access to IS processing or storing classified information after a determination has been made that the information is releasable to their country IAW the *National Disclosure Policy (NDP-1*). Access may be granted only to information under their direct control, limited to a specific program or project and limited to that described in the approved LAA. The foreign national must be supervised at all times by appropriately cleared U.S. personnel.

(3) Prior to being granted access to an IS, individuals will be briefed of their accountability requirements as outlined in paragraph 2-2b.

b. Personnel Exchange Program/Scientific Engineer Exchange Program/Foreign Exchange Personnel.

(1) Commanders may grant access to IS used to process or store classified information and/or SBU, provided the individual has been integrated into the DA work force and operating within the terms of certification outlined by a HQDA approved Delegation of Disclosure Authority Letter (DDL).

(2) Prior to being granted access to an IS, individuals will be briefed of their accountability requirements as outlined in paragraph 2-2b.

(3) Approval for specific information processed or stored should be coordinated

and approved through Foreign Disclosure channels.

(4) Specific user-IDs and passwords will be assigned to each individual for the period they are certified to the organization and require access. System access will be terminated upon expiration of the certification or departure from the organization, which ever is earlier.

(5) E-mail addresses should identify the individual as a foreign national.

(6) Additional specific guidance is contained in AR 380-10.

b. Foreign Liaison Officer.

(1) Prior to being granted access to an IS, individuals will be briefed of their accountability requirements as outlined in paragraph 2-2b.

(2) Access to IS may be granted to an LNO certified to the organization granting access in accordance with the terms of certification outlined by a HQDA approved DDL. Additional specific guidance is contained in AR 380-10.

(3) E-mail addresses should identify the individual as a foreign national.

c. Foreign Students.

(1) Prior to being granted access to an IS, individuals will be briefed of their accountability requirements as outlined in paragraph 2-2b.

(2) Access to IS used to process or store unclassified or SBU information is authorized provided specific user-IDs and passwords are assigned to each foreign student for the period they are assigned as students to the organization and require access. System access must be terminated upon completion of training requirements or upon departure from the organization, whichever is earlier.

(3) E-mail addresses should identify the individual as a foreign national.

e. Volunteer Workers.

(1) Prior to being granted access to an IS, volunteer workers will be briefed of their accountability requirements as outlined in paragraph 2-2b.

(2) A volunteer will not be granted access to IS used to process or store classified information.

(3) Prior to granting access, Commanders must be satisfied that the individual is suitable for the volunteer service.

f. Temporary Employees.

(1) Per OPM guidance, temporary employees and summer hires (under 120-day appointment) are not normally processed for a suitability investigation.

(2) Commands may require the individual to complete an SF 85-P to conduct a local suitability review prior to granting access to unclassified IS.

(3) Prior to being granted access to an IS, individuals will be briefed of their accountability requirements as outlined in paragraph 2-2b.

CHAPTER 2, SECTION VII:

2-18. Information Systems Media Protection Requirements

a. Refer to AR 380-5 and DOD 5200.1-R for specific guidance on protecting classified media.

b. Classifed output, either as hardcopy or softcopy, including documents maintained on an IS system, will be protected IAW AR 380-5 and DOD 5200.1-R.

2-19. Labeling and marking media

a. Removable storage media include magnetic tape reels, disk packs, diskettes, CD-ROMs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes and micro-cassettes, and any other device on which data is stored and which normally is removable from the system by the user or operator. All such devices bearing classified information must be conspicuously marked with the highest level of classification stored on the device and any special control notices that apply to the information using one of the labels specified below. As an exception, in the case of CD-ROMs, the label may be affixed to the sleeve or container in which the CD-ROM is stored. Other information normally provided by document markings (e.g., "classified by" and "declassify on" lines) shall be available

as follows:

(1) If the information is stored in readily accessible format on the device, it does not have to be marked on the outside of the device. As an example, if classified files or documents prepared with a word processor are stored on a floppy diskette, and each file bears its own declassification instructions as entered with the word processor, the diskette does not need to be marked with declassification instructions. This should be true with respect to most diskettes containing classified word processing files and documents, even though a few of them may not have all of the prescribed markings.

(2) If the required information is not stored in readily accessible format on the device, it must be marked on the outside of the device (normally with a sticker or tag) or placed on documentation kept with the device.

b. Standard Form (SF) Labels. If not marked otherwise, IS storage media and other items covered by this Section must be marked with the following labels:

(1) SF 706 - TOP SECRET
(2) SF 707 - SECRET
(3) SF 708 - CONFIDENTIAL
(4) SF 709 - CLASSIFIED
(5) SF 710 - UNCLASSIFIED
(6) SF 711 - DATA DESCRIPTOR

c. SF 711 should be used any time classified IS storage media are removed from the office in which they were created. There is no intention to require use of SF 710 in environments where no classified information is created or used. SF 709 should not be used if the appropriate classification label (SF 708, SF 707, or SF 706) is available.

d. Information that has been determined to qualify for Official Use Only (FOUO) status should be indicated by markings when included in documents and similar materials.

(1) Pages of documents that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom.

(2) Material other than paper documents (for example, slides, IS media, films, etc.) shall bear markings that alert the holder or viewer that the material contains FOUO information.

(3) When Sensitive But Unclassified (SBU) information is included in media/documents, they shall be marked as if the information were FOUO.

(4) Privacy Act media/documents will be marked as FOUO.

2-20. Clearing, purging, declassifying and destroying media. The procedures contained below meet the minimum security requirements for the clearing, sanitizing, releasing, and disposal of magnetic media. These procedures were extracted from the "Joint DODISS/Cryptologic SCI Information Systems Security Standards" which superceded Sup 1 to NSA CSS 130-1, the previous governing directive.

a. Media that has ever contained Cryptographic (CRYPTO) material cannot be sanitized at all, it must be destroyed. Media that has ever contained SCI, other intelligence information, or Restricted Data can not be sanitized by overwriting; such media must be degaussed before release.

b. Review of Terms. To better understand the procedures contained herein, it should be understood that overwriting, clearing, purging, degaussing, and sanitizing are not synonymous with declassificiation. Additionally, the following definitions should be reviewed:

(1) Clearing. Clearing is the process of eradicating the data on the media before the media is reused in an environment that provides an acceptable level of protection for the data that was previously on the media before clearing. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval. Clearing can be accomplished by overwriting or degaussing.

(2) Sanitizing (Also Purging). Sanitizing is the process of removing the data on the media before the media is reused in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing. In general, laboratory techniques cannot

retrieve data that has been sanitized/purged. Sanitizing may be accomplished by degaussing.

(3) Destroying. Destroying is the process of physically damaging the media to the level that the media is not usable as media, and so that there is no known method of retrieving the data.

(4) Declassification. Declassification is a separate administrative process whose result is a determination that given media no longer requires protection as classified information. The procedures for declassifying media require Designated Approval Authority (DAA) or Service Certifying Organization (SCO) approval.

(5) Periods Processing. A system is said to operate in a "Periods Processing" environment if the system is appropriately sanitized between operations in differing protection level periods, or with differing user communities or data. Provided the sanitization procedures between each protection level segment have been approved by the DAA/SCO based on guidelines from the data owner(s) or responsible official(s), the system need to meet only the security requirements of each processing period, while in the period. If the sanitization procedures for use between periods are approved by the DAA/SCO, the security requirements for a given period are considered in isolation, without consideration of other processing periods. Such sanitzation procedure shall be detailed in the accreditation support documentation package.

(6) Overwriting Media. Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method of clearing; however, the effectiveness of the overwrite procedure may be reduced by several factors, including: ineffectiveness of the overwrite procedures, equipment failure (e.g. misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps. Overwriting is not an acceptable method for declassifying.

(7) Overwriting procedures. The preferred method to clear magnetic disks is to overwrite all locations three (3) times (the first time with a random character, the second time with a specified character, the third time with the complement of that specified character).

(8) Overwrite verification. The overwrite procedure must be verified by the IASO or designee.

(9) Degaussing Media. Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

(10) Magnetic Media Coercivity. Magnetic media is divided into three types (I,II,III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained prior to executing any degaussing procedure.

(11) Types of Degaussers. The individual performing the physical degaussing of a component must ensure that the capability of the degausser meets or exceeds the coercivity factor of the media, and that the proper type of degausser is used for the material being degaused. The three types of degaussers are:

(a) Type I. Used to degauss Type I media (i.e., media whose coercivity is no greater than 350 Oersteds (Oe)).

(b) Type II. Used to degauss Type II media (i.e., media whose coercivity is no greater than 750 Oe).

(C) Type III. Used to degauss Type III media (i.e., media whose coercivity is no greater than 750 Oe). Currently, there are no degaussers that can effectively degauss all Type III media. Some degaussers are rated above 750 Oe, and their specific

approved rating will be determine prior to use.

c. Degausser Requirements. Refer to the current issue of the National Security Agency (NSA) Information Systems Security Products and Services Catalogue (Degausser Products List Section), for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to assure continued compliance with the appropriate specifications. National specifications provided a test procedure to verify continued compliance with the specifications.

d. Use of a Degausser. Once a degausser has been purchased and has become operational, the gaining organization must establish a "standard operating procedure (SOP)" explaining how it will be used.

e. Sanitizing Media. Tables 2-1 and 2-2 provide instructions for sanitizing data storage media and system components.

Table 2-1 Sanitizing Data Storage Media

Media Type	**Procedure(s)**
Magnetic Tape	
Type I	a or b
Type II	B
Type III	Destroy
Magnetic Disk Packs	
Type I	a or b
Type II	B
Type III	Destroy
Magnetic Disks	
Floppies	Destroy
Bernoullis	Destroy
Removeable hard disks	a or b
Non-removeable hard disks	a or b
Optical Disks	
Read Only (including CD-ROMs)	Destroy
Write Once, Read Many (WORM)	Destroy
Read Many, Write Many	Destroy
Procedures	
These procedures will be performed or supervised by the IASO	
a. Degauss with a Type I degausser	
b. Degauss with a Type II degausser	

Table 2-2 Sanitizing System Components

Type of Component	**Procedure(s)**
Magnetic Bubble Memory	a or b or c
Magnetic Core Memory	a or b or d
Magnetic Plated Wire	d or e
Magnetic Resistive Memory	Destroy
Solid State Memory Components	
Dynamic Random Access Memory (DRAM) (Volatile)	Destroy
If RAM is functioning	d, then e and i
If RAM is defective	f, then e and i
Static Random Access Memory (SRAM)	j
Programmable ROM (PROM)	Destroy (see h)
Erasable Programmable ROM (EPROM/UVPROM)	g, then c and i
Electronically Erasable PROM (EEPROM)	d, then i
Flash EPROM (FEPROM)	d, then i
Procedures	
These procedures will be performed or supervised by the IASO	
a. Degauss with a Type 1 degausser	
b. Degauss with a Type II degausser	
c. Overwrite all locations with any random character	
d. Overwrite all locations with a random character, a specifiied character, then it's complement	
e. Remove all power, including batteries and capacitor power supplies from RAM circuit board	
f. Perform three power on/off cycles (60 seconds on, 60 seconds off each cycle, at a minimum).	
g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3	
h. Destruction required only if ROM contained a classified algorithm or classified data	
i. Check with the IASPM/DAA/SCO to see if additional procedures are required	
j. Store a random unclassified test pattern for a time period comparable to the normal usage cycle.	

f. Destroying Media. Data storage media will be destroyed in accordance with DAA/SCO approved methods.

(1) Expendable Item Destruction. Expendable items (e.g. floppy diskettes) are not authorized to be released for reuse outside of the SCI community. If these items are damaged or no longer deemed usable, they will be destroyed. When destroying, remove the media (magnetic mylar, film, ribbons, etc.) from any outside container (reels, casings, hard cases or soft cases, envelopes, etc.) and dispose of the outside container in a regular trash receptacle. Cut the media into pieces (a crosscut, chipper/shredder may be used to cut the media into pieces) and then burn all pieces in a secure burn facility. If the Environmental Protection Agency (EPA) does not permit burning of a particular magnetic recording item, it will be degaussed, cut into pieces (a chipper/shredder preferred) and disposed of in a regular trash receptacle.

(2) Destruction of Hard Disks and Disk Packs.

(a) Hard Disks. Hard disks are expendable items and are not authorized to be released for reuse outside of the SCI community unless they have been degaussed and declassified. Each item is considered classified to the highest level of data stored or process on the IS in which it was used. If hard disks are damaged, or no longer deemed usable, they will be destroyed. If the platter(s) of the defective unit can be removed and the removal is cost effective, then destruction of a hard disk consists of dismantling the exterior case and removing the platter from the case. Local destruction of the platter consists of removing the magnetic surface by sanding, if environmentally allowed. If not allowed, contact your DAA/SCO for further instructions.

(b) Disk packs. Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If disk packs are damaged, or no longer deemed usable, they will be destroyed. Local destruction of the platter consists of degaussing or removing the magnetic surface by sanding if environmentally allowed. If not allowed, contact your DAA/SCO for further instructions.

g. Malfunctioning Media. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing will be reported to the Information Assurance Security Officer (IASO)/System Administrator (SA). The IASO/SA will coordinate the repair or destruction of the media with the IASM and responsible DAA/SCO.

h. Release of Memory Components and Boards. Prior to the release of any malfunctioning components the following requirements will be met in respect to coordination, documentation, and written approval. This section applies only to components identified by the vendor or other technically-knowledgeable individual as having the capability of retaining user-addressable data. It does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), that may be released without reservation. For the purposes of this section, a memory component is considered to be the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies. Unlike magnetic sanitization, clearing may be an acceptable method of sanitizing components for release (See Table 2-2). Memory components are specifically handled as either volatile or nonvolatile, as described below.

(1) Volatile Memory Components. Memory components that do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data are considered volatile memory components. Volatile components that have contained extremely sensitive or classified information may be released only in accordance with procedures developed by the IASM, or designee, and stated in the accreditation support document package. A

record must be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.

(2) Nonvolatile Memory Components. Components that do retain data when all power sources are discontinued are nonvolatile memory components – including Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM), and their variants, that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components (e.g., removable/non-removable hard disks) may be released after successful completion of the procedures outlined in Table 2-1. Failure to accomplish these procedures will require the IASM, or designee, to coordinate with the DAA/SCO to determine releaseability.

(3) Other Nonvolatile Media:

(a) Visual Displays. A visual display may be considered to be sanitized if no sensitive information is etched into the visual display phosphor. The IASO should inspect the face of the visual display without power applied. If sensitive information is visible, destroy the visual display before releasing it from control. If nothing is visible, the IASO/SA shall apply power to the visual display; then vary the intensity from low to high. If sensitive information is visible on any part of the visual display face, the visual display shall be destroyed before it is released from control.

(b) Printer Platens and Ribbons. Printer platens and ribbons shall be removed from all printers before the equipment is released. One-time ribbons and inked ribbons shall be destroyed as sensitive material. The rubber surface of platens shall be sanitized by wiping the surface with alcohol.

(c) Laser Printer Drums, Belts, and Cartridges. Laser printer components containing light-sensitive elements (e.g., drums, belts, and complete cartridges) shall be sanitized before release from control.

(1) Elements containing information that is classified, but is not intelligence information, can be considered sanitized after printing three printer font test pages.

(2) Elements containing intelligence information shall be sanitized in accordance with the policy contained in the Director of Central Intelligence Directive (DCID) 1/21.

i. Release of Systems and Components. The IASM, or designee, shall develop equipment removal procedures for systems and components. These procedures should be stated in the accreditation support documentation package. When such equipment is no longer needed, it can be released if:

(1) It is inspected by the IASM or designee. This inspection will assure that all media, including internal disks, have been removed or sanitized.

(2) A record is created of the equipment released indicating the procedure used for sanitation and to whom the equipment was released. The record of release shall be retained for a period prescribed by the DAA/SCO.

(3) Procedures specified by the DAA/SCO are used.

j. Documenting IS Release or Disposal. The National Security Agency/Central Security Service (NSA/CSS) Form G6522, or similar form/documentation, will be used to document the local release or disposal of any IS or processing component.

2-21. Non-Removable Storage Media**.** System managers shall ensure that ISs, including word processing systems, provide for classification designation of data stored in internal memory or maintained on fixed storage media.

CHAPTER 2, SECTION VIII: NETWORK SECURITY (DEV BY COMMITTEE # 4)

2-22. General Network Security

a. Network Security requires the protection of networks and their services from unauthorized modification, destruction, or disclosure, and provides assurance that the network performs its critical functions correctly and there are no harmful side effects.

b. Types of Networks to be protected are Local Area Networks (LAN), Metropolitan Area Networks (MAN), and Wide Area Networks (WAN). The LAN covers a limited geographic area, is generally owned and administered by one group, with a limited number of users, no common carrier communications, and a high transmission rate. A MAN covers an area larger than a LAN, and is sometimes referred to as a campus network. A WAN covers a wider geographic area.

c. Functional classifications of Networks: For the purpose of applying standards and identifying responsible officials, the following classifications of a network shall be considered:

(1) Interconnected Accredited AIS (IAA) is an interconnection of separately created, managed, and accredited, AIS. An IAA consists of multiple systems accredited to operate within a range of values and may include systems that do not fall under DoD directives. The following security provisions are applicable to the IAA.

(a) There shall be a single identified network Designated Approving Authority (DAA) for multiple individually accredited AIS. An example is DISA having overall control of the Defense Information Systems Network (DISN) security parameters. There are circumstances when a central focal point cannot be identified, in this latter case, each individual AIS DAA must establish procedures to protect the data contained in the AIS and to ensure that only authorized data is transmitted on the IAA network.

(b) The DAA of the individual AIS must specifically approve connection of the AIS to an IAA. This approval will be part of the AIS accreditation. Approval will be granted after assessing the additional risks involving the potential exposure of data within the larger community of AIS infrastructure.

(c) The DAA approval will include a description of the classification and categories of information that can be sent over the IAA. Unless the AIS is accredited for multilevel operations and can reliably separate and label data, the AIS is assumed to be transmitting the highest classification level of data present on the system during network connection.

(d) The DAAs of the participating AIS and the DAA of the overall network (if one has been designated) will sign a Memorandum of Understanding (MOU). In those cases where standard procedures for connecting to the network have been defined by a DAA, those procedures, coupled with the approval of the DAA to connect, will serve as the MOU.

(e) Connections between accredited AIS must be consistent with the mode of operation, sensitivity level or range of levels, and any other restrictions imposed by the accredited AIS.

(f) Connections to unaccredited AIS (that is, from other agencies or non-governmental entities) are authorized, but only non-sensitive unclassified and SBU data may be transmitted to and from such AIS. Data that is SBU must be afforded the proper protection requirements (data confidentiality, data integrity, and data availability) to ensure compliance IAW AR25-IA.

(2) A Single Trusted System (STS) is one which the network is accredited as a single entity by one DAA. The STS is normally appropriate for local area networks (LAN), but can be applicable to wide area

networks (WAN) for which a single agency or official has responsibility. The STS view is one in which the network is accredited as a single entity by one DAA. The following security provisions apply to the STS view of a network:

(a) The STS view of a network provides the greatest probability that security will be adequately addressed in a network, and it will be used in lieu of the IAA view whenever possible.

(b) Sensitivity category and mode of operation of the STS network will be determined as described in AR25-IA. Minimum requirements of AR25-IA are fully applicable, including the minimum trusted class requirement when the network operates in other than the dedicated mode. Part I of the NCSC-TG-005 can be used to determine how to interpret DOD 5200.28-STD for an STS network. Additionally, part II of the NCSC-TG-005 describes three other security services. Each service has three sub-elements that must be addressed in the STS network accreditation. These services with sub-elements are:

(1) Communications integrity - (authentication capability, field integrity, and ability of the network to enforce non-repudiation of a message);

(2) Denial of service characteristics - (continuity of operations, protocol-based protection against denial of service, and adequacy of network management);

(3) Compromise protection – (data confidentiality, traffic flow confidentiality, and the ability to route transmissions selectively in the network.)

c. The security services described above can be addressed only in a subjective manner and may not be applicable or desirable in all situations. The IASOs and network DAAs must consider each of them in defining their network security requirements and develop countermeasures for those services that are required but not present.

2-23. Network Systems Security Controls

a. Threats and Vulnerabilities. IA personnel shall ensure networks are protected from both hostile and benign threats to ensure the availability, confidentiality, and integrity of data.

(1) Availability prevents resources from being deleted or becoming inaccessible. This applies to information, networked machines and other aspects of the technology infrastructure. The inability to access those required resources is called a “denial of service.” Intentional attacks against computer systems often aim to disable access to data, and occasionally the aim appears to be the theft of data. These attacks are launched for a variety of reasons including both political and economic motivations. In some cases, electronic mail accounts are flooded with unsolicited messages, known as spam.

(2) Confidentiality is the concept that information is unavailable to those who are unauthorized to access it. Strict controls must be implemented to ensure that only those persons who need access to certain information have that access. In some situations, such as those with confidential and secret information, people should only have access to that data which is necessary to perform their job function. Many computer crimes involve compromising confidentiality and stealing information.

(3) Integrity ensures that information cannot be modified in unexpected ways. Loss of integrity could result from human error, intentional tampering, or even catastrophic events. The consequences of using inaccurate information can be disastrous. If improperly modified, data can become useless, or worse, dangerous. Efforts must be made to ensure the

accuracy and soundness of data at all times.

b. A threat may be defined as an event or method that can potentially compromise the integrity, availability, or confidentiality of information systems. Threats to networks and connected systems can be generalized into the following three categories

(1) Hostile intelligence services or business equivalents collecting information through unauthorized access.

(2) Fraud through illegal access to data causing denial of service or loss of confidentiality.

(3) Deliberate or inadvertent error by authorized or unauthorized users. Computer viruses, malicious code, and programs designed to bypass security programs are examples of deliberate error. Accidental erasure of data by an authorized user is an example of an inadvertent error.

c. Depending on the site, there will be more specific threats that shall be identified and addressed.

d. IA personnel shall identify system vulnerabilities through which identified threats could adversely affect the network or its associated assets.

(1) System vulnerabilities are weaknesses in design, system security procedures, implementation, and internal controls that could be exploited by authorized or unauthorized users. Vulnerabilities can occur as a result of the lack of security safeguards or ineffective safeguards

(2) Conducting a risk analysis is an excellent tool for identifying vulnerabilities and providing the appropriate safeguards.

(3) Vulnerability Assessments are routinely performed by the applicable ACERT/RCERT. Commanders may request a VA be conducted on their installation's network. Formal request indicating intent and scope must be submitted to the Army DCSOPS and DCSINT for approval. MACOMs may require staffing the request through their IAM prior to submission to DA. Upon gaining DCSOPS/DCSINT approval, the ACERT will coordinate all further activity with the requesting commander or his/her designee. The actual process of the Vulnerability Assessment is further defined under CDAP. Results of any Vulnerability Assessment are released only to the requesting commander. That commander may share the results with anyone he/she chooses. Commanders are reminded that the results are sensitive in nature and as a minimum, should be treated as "For Official Use Only".

e. Computer Defense Assistance Program (CDAP). The proponent agency for the CDAP is LIWA through its ACERT/(RCERT)). LIWA draws its authority for CDAP under two separate regulations AR 25-IA and AR 380-53. That portion of the CDAP, which covers mapping the network and scanning for vulnerabilities, is derived from AR 25-IA. AR 380-53 governs the portion of the CDAP, which pertains to verification of detected vulnerabilities and actual penetration testing of the network. AR 380-53 concerns penetration testing, which concerns security testing in which evaluators attempt to circumvent the security features of an automated information system based on their understanding of the system design and implementation. The purpose of penetration testing is to confirm and demonstrate, through exploitation, the degree of the automated information system vulnerabilities.

f. To achieve network security the following should be taken into consideration in order to control and protect Network resources.

(1) Designate a certified IA person to assign and manage user ids and passwords, monitor audit trail reports, configure/manage network hardware and software, and ensure the compliance with software licensing agreements.

(2) Establish a physical security policy to restrict access to network devices.

(3) develop a password control policy.

(4) Develop a policy requiring users to secure their systems when left unattended.

(5) Secure network cabling. Every effort shall be made to lock and restrict access to interconnection junction areas, such as wire closets where all network circuits begin, end, and interconnect.

(6) Develop and maintain up-to-date cabling diagrams.

(7) Implement Encryption as required.

(8) Develop backup and recovery procedures for network devices.

(9) Maintain up-to-date documentation of the network hardware and software.

(10) Have backup power for critical network devices. Install an uninterruptible power supply (UPS). Install surge protection devices on all network devices.

(11) Provide security and awareness training for users.

(12) Initiate background and reference checks prior to contracting with outside consultants for installing or troubleshooting networks.

(13) Consider prohibiting the use of remote network software that operates programs and accesses peripherals on a remote system via a modem.

(14) Develop an anti-virus protection and reporting program.

(15) Restrict use of modems in systems that are concurrently connected to the network. Local DAA may consider exceptions based on operational requirements, but shall document those exceptions and take any necessary measures to negate risks to the network.

(16) Install a dedicated virus monitoring, detection, and purging software package.

(17) Monitoring. SA/NA can perform IA and information systems and network functions in order to keep their own AIS infrastructure operational and secure. This includes performing vulnerability analysis of the operating systems of the AIS directly under the control of the system and/or network administrator. AR 25-IA outlines specific capabilities and restrictions that a SA and/or NA can or cannot perform as pertains to ISS monitoring.

g. Virus Protection

Army networks and systems are vulnerable to malicious codes (viruses, trojan horses, worms, etc) that can cause destruction of information or denial of service. The introduction of malicious codes can cause significant security breaches; sensitive information can be captured and transmitted, critical information can be modified, and the software configuration of a computer can be changed to permit subsequent intrusions.

(1) (1) Possible sources of viruses

1. (a) Software introduced into or used on the system by an insider/outsider who had access to the system.

(b) Software used at home on infected system.

(c) Software purchased from a vendor who has an infected production system.

(d) Infected software from the Internet

(e) Software intentionally infected by a disgruntled user.

(2) To minimize the risks of viruses, the following countermeasures should be implemented:

(a) Ensure computers have the most recent versions of the anti-virus software.

(b) Take the multi-level approach to virus detection by installing one anti-virus package on the workstations and a different anti-virus package on the servers.

(c) Virus definitions should be updated at least weekly.

(d) Train the users to help prevent malicious code from being installed on their workstations and transmitted to the servers. This includes training users to scan all software, downloaded executable files and email attachments before being introduced into their systems.

(e) Train users to recognize virus symptoms, report them to the IASO, and run appropriate virus eradication tools.

2-24. Security Protection between Networks. Protection from External networks (that portion of the network which is outside the installation and/or activities controls)

a. The DISC4, as the Army Chief Information Officer (CIO) is responsible for implementing procedural and materiel protective measures, developing plans and policies, developing and monitoring training, and validating requirements to protect command, control, communications and computer capabilities (C4). The primary plans for enhancing the overall network and systems security posture for the Army are the Protection Plan for Force XXI Information Systems for the tactical force and the Network Security Improvement Program (NSIP) for the sustaining base. Together they implement a seamless, "Defense-in-Depth" strategy to protect against unauthorized intrusions from the sustaining base to the deployed force. They are consistent with guidance in the Office of the Secretary of Defense (OSD) Defense-Wide Information Assurance Program (DIAP) and Defense Information Systems Agency (DISA), Joint Staff, and Service information assurance (IA) efforts.

b. Protection Plan for Army XXI Information Systems. This plan is a strategy for integrating systems protection into the design of battlefield information systems, networks, and the network infrastructure of the digitized force. It is also a plan for assessing the extent to which the information systems protection process, coupled with appropriate tactics, techniques, and procedures, provides anticipated levels of protection. It employs a risk management approach, which recognizes that risks to the C4 assets of Army XXI units cannot be totally prevented or avoided, but can be managed by employing like technology from the sustaining base through the tactical force.

c. Network Security Improvement Program (NSIP). The NSIP identifies responsibilities (for both active and reserve components) and sets forth a managed, phased approach for improving the Army's security posture by establishing policy and procedures, identifying enabling technologies, and integrating IA security tools into the C4 architecture for the War-fighter's power projection platforms. The NSIP builds on a foundation of workstation and server-based security, hardened infrastructure, and new technology acquisition, to include near-real-time network router monitoring, enterprise licenses for intrusion detection system (IDS) and firewall technologies, upgrading Domain Name Service (DNS) server security, eliminating "backdoors" into the Army NIPR Net, strong identification & authentication (I&A) of dial-in connections, and integration of new technologies (e.g., biometrics) in accordance with OSD and DISA policy.

d. Global Intrusion Detection Monitoring.

(1) In accordance with Deputy Secretary of Defense (DEPSECDEF) guidance to establish IDS capabilities, DISC4 tasked the Army Signal Command (ASC) to develop a worldwide 24 hours a

day, seven days a week automated IDS monitoring capability.

(2) The DISC4, in coordination with the DCSOPS and DCSINT, (the C2 Protect Triad) has mandated an Army-wide Computer Emergency Response Team (ACERT) infrastructure, under the Land Information Warfare Activity (LIWA). The infrastructure consists of an ACERT Coordination Center and regional and local CERTs to identify and track anomalies that indicate intrusions into Army information systems and to take appropriate actions against intruders. The LIWA maintains a Red Team and Computer Defense Assistance Program (CDAP) capability to assess the IA vulnerability status of the tactical force and sustaining base installations.

e. Positive Control/Information Assurance Vulnerability Alert (IAVA). IAVA implements the DEPSECDEF positive control requirement and ensures the Army's capability to document that corrective actions have been accomplished. MACOMs are required to identify a C2 Protect/IA officer (IAO) for their commands who are responsible for ensuring that their MACOMs comply with Army issued information systems security alerts and advisories. MACOM IAOs are required to identify system administrators/network managers responsible for implementing corrective actions identified in Army issued alerts and advisories for all relevant networks and systems within their command. The LIWA's ACERT provides the verification capability.

f. Training and Certification. A key to successful implementation of the NSIP is increased and enhanced training and certification of all personnel. IA training is conducted at the U.S. Army Signal School, by mobile training teams, at regional and national conferences and workshops, and enterprise licensed computer based training.

g. NSIP initiatives include:

- Proxy Servers
- Security Routers
- Demilitarized Zone (DMZ)
- Firewalls
- Elimination of "Back Doors"
- Intrusion Detection Systems (IDS)
- 3 Tier Domain Name Service (DNS)
- Worldwide Global Network View (WWGV WWNV)
- Public Key Infrastructure (PKI)

(1) PROXY SERVERS

(a) A proxy server provides a number of security enhancements. It allows sites to concentrate services through a specific host to allow monitoring, hiding of internal structure, etc. This funneling of services creates an attractive target for a potential intruder. The type of protection required for a proxy server depends on the proxy protocol in use and the services being proxied. The general rule of limiting access only to those hosts which need the services, and limiting access by those hosts to only those services, is a good starting point.

(b) Simple Network Management Protocol (SNMP), Port 161,162) - SNMP is an Internet protocol for centrally managing network equipment. It is used to monitor and configure network devices such as routers, bridges, hubs, and hosts. Port 161 is used for commands and port 162 is used for alarms from network devices. SNMP daemons will be used to manage resources internal to a LAN (inside the firewall). SNMP queries through the firewall are not permitted. The major security issue is that someone might be able to take over your equipment and reconfigure it. Recommendation is to block port 161, and open port 162 only if you monitor outside equipment, and then open only to your SNMP server.

(c) HyperText Markup Language (HTML) protocol allows network users unrestricted viewing of WWW using an Internet browser. The public will only be able to view information approved for public viewing and located on the WWW server.

(d) Simple Mail Transfer Protocol (SMTP), Port 25 - SMTP is the protocol used to transfer e-mail messages between mail servers on the Internet. SMTP is a store-and-forward system in which the SMTP server looks at the address of the e-mail message, and if it is a local address, it stores the message in the user's mailbox. If it is not a local address, it forwards the message. Recommendation is to allow use of port 25, but only to the e-mail server.

(e) File Transfer Protocol (FTP), Port 20 and 21, allows network users to query and obtain information from other hosts outside a network. It may be necessary to provide an electronic security advisory to the remote FTP host(s) because there is a possibility that the FTP daemon can be compromised. An example is when the Windows NT proxy server intercepts the user's FTP userID and password, Windows NT generates a userID and password that is proxied to the remote host. It is recommended that you do not allow incoming FTP requests from the outside. FTP should be allowed to go through the firewall from the inside to the outside. The transaction should be audited.

(2) Routers. There are three basic types of routers in existence on most Army installations. Those three types and their functions are:

(a) Security (or screening). The security router is owned, operated, and maintained by the Army Signal Command (ASC) and acts as the initial line of defense for the installation. This router protects Army networks through implementation of an Access Control List (ACL). This ACL is centrally managed by ASC and it's Theater Network Operations Centers (TNOCs) with input from the Army Computer Emergency Response Team (ACERT). The purpose of the ACL is to provide a means of blocking suspect networks from accessing Army networks. The ACL can also be configured to protect the Army network from certain types of attacks (e.g. NETBUS) where a specific protocol or port is used as the basis of the signature.

(b) Gateway (or premise). On most Army installations, the gateway router is owned, operated, and maintained by the Army Signal Command (ASC). This router provides a central focal point on the installation for interconnecting diverse local area networks. All remote connections exiting the installation will be connected to this router and must be approved by the appropriate ASC element. The approval process begins with submission of a Request for Service (RFS).

(c) Installation Infrastructure. Typically owned and operated by the installation DOIM. Under some circumstances and with approval of the installation DOIM, some of these routers may be owned and operated by users. Routers under this category are normally intended to extend the LAN (or MAN) to reach remote enclaves of users. In a non-CUITN (Common user installation transport network) or ATM LAN, routers may also be deployed to segment the network into separate collision domains. All such routers, regardless of ownership, will be subject to centralized (at the installation level) configuration management and will be periodically reviewed by the installation IANM/IASO.

(d) The following procedures shall be used to improve security on routers and other network devices:

(1) Access Control Lists (ACL)

(a) ACLs are centrally managed by ASC for all security and premise routers

(1) ASC determines what IP addresses are to be blocked

(2) ACERT may recommend addresses to be blocked

(3) RCERTs may recommend addresses be blocked based on results of IDS analysis or other indicators

(4) Theater Network Operations Center (TNOC) implement all changes to ACL (TNOCs act as the ASC agent within a given theater of operations)

(5) Local Network Operations Center (NOC) (those with delegated authority) may add additional addresses to be blocked based on local policy or trends in activity. Local NOC will not over-ride (or supercede) changes implemented by the TNOC.

(b) More than one ACL may co-exist on the router. The most restrictive ACL (that which incorporates all ASC directed blocks) will be assigned to the specific interface connecting to the NIPRNET.

(c) ACLs will be verified periodically to validate authenticity and accuracy. Each responsible agency will establish policy to determine how the ACL is validated and how often it should occur. As a minimum, the ACL should be reviewed monthly.

(d) IP accounting logs will be reviewed routinely for any attempts to access the system from a blocked IP address. Such attempts will be reported to the appropriate RCERT.

(e) Ensure a back-up copy of the router configuration is available at all times. This will be used to validate/verify integrity of the configuration when an anomaly is encountered. Back-up copy can be downloaded to a secure Trivial File Transfer Protocol (TFTP) server.

(f) All changes to the router configuration shall be fully documented

(2) Services

(a) TNOCs, NOCs, and Network Administrators should determine the minimum services required for optimum performance of the network. Services not required, shall be disabled.

(b) Telnet and FTP should be restricted to those personnel responsible for managing/maintaining the devices. Those accessing the device through these services should be subjected to strong authentication and all activity logged.

(3) Protocols

(a) Internet Control Message Protocol (ICMP) should be disabled providing that in so doing, network performance/functioning is not adversely affected. Disabling ICMP will protect the router from some denial of service attacks. It will also deny the use of ping and tracert as troubleshooting tools. Through judicious use of an ACL, this protocol can be permitted for specific users that need the troubleshooting tools.

(b) Default SNMP community strings will be removed. If the device requires management through SNMP, create a new string and assign specific permissions (e.g. Read-Only (RO) or Read-Write (RW)).

(c) Provide the SNMP string only to those network administrators that have a need for it.

(4) Logon & Passwords (Routers and Switches)

(a) Authorized users must logon to the device with a unique user-id. This should be accomplished through use of a program similar to TACACs+ (for Cisco routers).

(b) User passwords (TACACS+) shall conform to policy and procedures detailed in section on passwords.

(c) The “Enable” password will follow the same guidelines (outline DA PAM) regarding structure and minimum length. Enable passwords for security and premise routers will be maintained on file at the appropriate TNOC.

(d) Access to routers will be allowed only from known IP addresses.

(5) Switches (Internetworking Devices)

(a) Controlling access to switches is essential to overall network security. If an unauthorized user gained access to a switch on the LAN, they could effectively turn off access to all other users. Additionally, it would provide a potentially unobserved (or trusted) connection point into the enclave.

(b) (b) Two specific methods of controlling access are:

(1) SNMP (a) Default SNMP community strings will be removed. If the device requires management through SNMP, create a new string and assign specific permissions (e.g. RO or RW).

(b) Provide the SNMP string only to those network administrators that have a need for it.

(2) Logon & Passwords (Switches)

(a) Passwords shall conform to policy and procedures detailed in section on passwords.

(b) The "Enable" or "super-user" password will follow the same guidelines regarding structure and minimum length.

(3) DMZ. The Demilitarized Zone (DMZ) is a buffer area between the security router and the gateway router. The DMZ is typically a publicly accessible area where an Internet server is located. The DMZ provides the mechanism to allow visitors access to the publicly accessible systems, while protecting the rest of the network from unauthorized access. The DMZ is further protected through use of a firewall and/or proxy server.

(4) Firewalls. A firewall provides boundary protection and allows computer network traffic to flow according to rules established in a security policy. Traditionally, the firewall has been viewed as the first element in security-in-depth for the installation's information system. Router filters and intrusion detection devices are often used in front of the firewall to work in combination with the firewall. These devices may be viewed as part of the firewall system. The current Army plan is to provide intrusion detection, firewall-like technology, and a proxy server to protect the initial boundary of each post. Commercial firewalls are still considered useful within each Army post for protecting more sensitive LANs like financial, medical, and personnel. Refer to (Appendix D) for further guidance.

(5) "Back Doors". Connectivity into the installation topology that is not connected IAW with Army Information Assurance (IA) standards. The issue is whether or not a connection is protected. There are five categories of backdoors:

- Circuits that are Army purchased and managed
- Network level connections with a Commercial Internet Service Provider (ISP)
- Point-to-Point connections between Army installations or between Army and Facilities, e.g., contractors that may be connected to the Internet or NIPRNET.
- Dial-in capabilities not currently using identification and authentication servers
- Dedicated network circuits that support specific functions (hereafter referred to as "functionals") with separate connections to the NIPRNET e.g., the Defense Research and Engineering Network (DREN)

(6) Intrusion Detection Systems (IDS). The IDS operates on a Unix and NT platform and utilizes a commercial off the shelf (COTS) software package known as RealSecure. This package provides the means of examining packets of information in transit looking for known attack signatures.

(7) 3 -Tier Domain Name Service (DNS). The new DNS design standardizes DNS and Internet Protocol Management (IPM) system hardware, software, and processes resulting in a validated, protected DNS Infrastructure maintained under centralized configuration management and security monitoring.

(a) Protected Domain Name System (DNS). The DNS function relates domain names to IP addresses and IP addresses to domain names and is an important component of the Army's protected backbone services in support of Internet processing. The current U.S. Army DNS architecture uses a diverse range of hardware and software platforms. The purpose of the U.S. Army Network Security Improvement Program Protected DNS is to establish a protected Army-wide DNS infrastructure. The protected DNS provides unclassified non-tactical DNS support to the active Army, the Army National Guard, the U.S. Army Reserves for all mission-related and administrative processes.

(1) Each non-tactical DNS server, new and existing, is part of the operational process that restricts unauthorized access to Army DNS information, monitors/reacts to DNS intrusion attempts, and prevents corruption or interruption of the information transport enabled by DNS.

(2) The protected DNS standardizes DNS and the Internet protocol management (IPM) system hardware, software, and processes resulting in a validated, protected, DNS infrastructure under centralized configuration management and security monitoring. The protected DNS and its associated processes extend to all Army facilities and include all protected DNS Army servers (Tier 0, Tier 1, Tier 2, and Tier 3 DNS servers).

(b) Central management of the DNS will be performed by authorized Theater Network and Systems Operations Centers (TNSOCs) with the support operationally integrated Regional Computer Emergency Response Teams (RCERTS) in CONUS, Europe, Pacific, and Korea. Subdomain DNS management will continue to be done by the DNS domain managers currently in place. Subdomain authorization will continue to be managed and controlled by USASC as the Army Domain Manager.

(c) Centralized management of the Army Domain includes Information Assurance/Vulnerability Alert (IAVA) compliance, worldwide monitoring of DNS intrusion detection and information security requirements, and configuration management of the protected DNS common operating environment by U.S. Army Signal Command.

(d) The Protected DNS architecture and associated common operating environment supports DNS in a layered structure.

(1) The 'Tier 0' layer supports external DNS queries from the public Internet and is designed to reduce the availability of unnecessary information associated with internal Army DNS assets. Internal Army DNS assets support the Tier 1, 2, and 3 layers. Tier 0 DNS servers are collocated with each TNSOC.

(2) Tier 1 servers provide centralized support to the regional Tier 2 servers. Tier 1 DNS servers are collocated with each TNSOC.

(3) Tier 2 servers are the authoritative primary servers for the Army subdomains they support and are geographically distributed to provide robust, regional DNS support to Army DNS users. Tier 2 servers are placed within the installation’s information security public access zone and are centrally monitored, maintained, and controlled by their supporting TNSOC. No change or relocation of Tier 2 servers is authorized without prior coordination with HQ, USASC.

(4) Tier 3 servers are normally internal to the installation and provide predominantly local DNS support. Tier 3 servers are a formal extension of the protected DNS and

will be monitored by their supporting TNSOC for IAVA compliance and adherence to DNS policies. Owning organizations will provide host based intrusion detection monitoring for these servers. Intrusions will be reported in accordance with IAVA procedures.

(5) Worldwide Global Network View (WWNGV). WWNV is an AIS with platforms in the CONUS, Pacific, Korea, and Europe Theater Network Systems Operation Centers (TNSOC) that provides the Army Commanders, global view status of Non-Classified but Sensitive Internet Protocol Router Network (NIPR Net) and Secured Internet Protocol Router Network (SIPR Net). WWNV is fielded at each TNSOC, which provides an overall picture of the locations and the products that make-up the WWNV. Each TNSOC has its own WWNV configuration to publish a web site for its Theater status, both on the NIPR Net and SIPR Net.

(9) Public Key Infrastructure (PKI) - PKI provides user identification and non-repudiation, authentication, and data integrity through digital signatures plus data privacy through encryption for programs, applications, and messaging. Public Key Infrastructure will provide the framework and services for the generation, production, distribution, control, and accounting of public key certificates. The initial Public Key Infrastructure system will allow Army members to register for and obtain digital signature and encryption keys. As business applications such as the Defense Travel System expand within the Army, there will be a growing reliance upon the Public Key Infrastructure to authenticate and secure electronic transactions

(10) Connections to unaccredited AIS (that is, from other agencies or non-governmental entities) are authorized, but only non-sensitive unclassified and SBU data may be transmitted to and from such AIS. Data that are SBU must be afforded the proper protection requirements (data confidentiality, data integrity, and data availability) to ensure compliance with Security -related requirements.

2-25. Protection from Internal Networks – Portion of the network that is directly controlled by the installation/activity

a. Trusts will be established in accordance with the installation Information System Architecture. There will be no trusted relationships established with any other domains or networks until they are approved by the Designated Approving Authority (DAA). This approval will be part of the AIS accreditation. It will be made only after accessing the additional risks involving the potential exposure of data within the larger community of AIS infrastructure. The DAA has authority to direct the dissolution of an established trust relationship in the event of a known or suspected compromise.

(1) The DAA's approval will include a description of the classification and categories of information that can be sent over the IAA. Unless the AIS is accredited for multilevel operations and can reliably separate and label data, the AIS is assumed to be transmitting the highest level of data present on the system during network connection.

(2) The DAA's of the participating AIS and the DAA of the overall network (if one has been designated) will sign a Memorandum of Understanding (MOU). In those cases where standard procedures for connecting to the network has been defined by the DAA, those procedures, coupled with approval of the DAA to connect, will serve as the MOU.

b. Connection between accredited AIS must be consistent with the mode of operation, sensitivity level or range of levels, and any other restrictions imposed by the accredited AIS. National Computer Security Center - Technical Guidance (NCSC-TG) - 005 contains additional restrictions that apply to connecting AIS to an IAA when the

AIS is accredited in the multi-level or compartmented mode.

(1) Remote Devices and Remote Access

(a) Remote terminal devices must be secured consistent with the mode of operation and information that the remote terminal is authorized to access.

(b) Army dial-in users will be required to migrate to an authentication system that will authenticate all dial-in operations with a unique user-id and password, that is compliant with the remote authentication dial-in user system (RADIUS) standard. The standards for such a system are:

(1) All dial-in operations will be authenticated with a unique user-id and password. Passwords shall be at least eight alphanumeric characters and reflect the current army password expiration policy of 6 months.

(2) Authentication systems supporting dial-in capabilities will migrate to the Joint Technical Architecture (JTA) compliant RADIUS standard. The RADIUS software shall be configured for accounting. Accounting logs will at a minimum show who logged in, when they logged in, and be stored for a year.

(3) All authentication servers will be protected with a host-based IDS. Users are responsible for operating and auditing the IDS results.

(4) The MACOM Information Assurance Program Manager(IAPM) will be responsible for reporting the location/IP address/hardware platform and version of OS of authentication servers to the ODISC4.

(5) All authentication servers will be remotely audited to ensure all Army IA standards are met. Recommend that users place authentication servers in a DMZ. ODISC4 will coordinate the remote configuration audits with the MACOM IAPM.

(c) If necessary, users must upgrade local terminal servers to be RADIUS compliant. Cisco terminal servers running IOS 11.2 or greater are RADIUS compliant. The army DISN router program upgraded the old Cisco ASM terminal servers to Cisco 5200 terminal servers. The old Cisco ASM terminal servers cannot run IOS 11.2 and must be upgraded or removed from operation. Microsoft RAS must be configured to allow TCP/IP or IPX clients access only to the local network. User dial-in accounts will be configured such that only access to a particular host computer will be allowed, and that users can not move from one service to another during a session. Passwords to use the RAS must be encrypted. Microsoft remote access servers in the DMZ configured for RADIUS and host-based IDS are the only exceptions where wide-area NIPRNET access is allowed for dial-in RAS users.

(d) Dial-in systems can be an exploitable entry point into the information backbone. DOIMs and users must ensure that any dial-in systems that are connected to the installation data network that they own or operate adhere to these standards. If they do not they must be disconnected. Those systems that are not owned or operated by the post, camp or installation DOIM and are not willing or able to meet army standards must be reported to the ODISC4.

(e) Stand alone dial-back modems and modem systems that authenticate using RADIUS are the only allowable modems. Without aggressive action, dial-in systems and stand-alone modems will continue to be a potential backdoor for unauthorized intruders.

(f) AIS with remote terminal access containing classified data will have a "time-out" protection feature that automatically disconnects the remote terminal from the computer after a predetermined period has passed without communication between the

terminal and the computer. The system should make periodic checks to verify the disconnect is still valid. The automatic disconnect must be preceded by a clearing of the remote terminal's screen followed by the recording of an audit trail record for the System Administrator to use. The time period should not exceed 15 minutes but may vary depending on the sensitivity of the data, the frequency of use and location of the terminal, the strength of the audit mechanism, and other physical or procedural controls in place. The time-out feature is not required if the accreditation authority determines the AIS must remain active because it is being used as a communications device. However, physical security for the terminal will meet the requirements for storage of data at the highest level that could be received at the terminal.

(g) Systems that process classified or SBU information will limit the number of user log-on attempts to three before denying access to that user. Users will not be re-instated until the appropriate IA personnel has verified the reason for failed log-on attempts.

(2) Identification, authentication, and encryption technologies will be employed when accessing networks.

(a) Identification is used to verify the identity of a system, originator, or individual prior to allowing access to a system, or specific categories of information within the system. The most common form of identification is the user ID. Such controls may also be used to verify that only authorized persons are performing certain processing activities on the system.

(1) Organizations shall require users to identify themselves uniquely before access is allowed on the system.

(2) All network devices shall be identified by a unique IP or MAC address.

(3) Systems shall internally maintain the identity of all active users and be able to link actions to specific users (See Audit trails)

(4) Organization shall ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting departed users.

(5) User Accounts that are inactive for 30 days or more shall be disabled.

(b) Authentication is the means of establishing the validity of a user's claimed identity to the system. There are three means of authenticating a user's identity, which can be used alone or in combination:

(1) Something a user knows, such as password, PIN, or cryptographic key.

(2) Something a user possesses, such a FORTEZZA card or Smart Card.

(3) Physical characteristics (biometrics). A few means of authentication are one-time passwords, Kerberos, PGP, PKI, Biometrics.

(c) File Encryption. Install and configure file encryption capabilities for sensitive data. Some operating systems provide optional file encryption; there are also third party encryption packages available. These may be useful if the operating systems access controls are insufficient for maintaining the confidentiality of file contents. This can be the case if the operating system provides few or no access control features, or when the relationships among categories of files and users are so complex that it would be difficult to use only access controls to administer the security policy. This recommendation pertains only to encryption of files stored on the computer itself.

(d) Network Encryption. Classified and SBU information will be transmitted only by secure means. When information transits an area not under access controls as stringent as required for that classification of the information, it will be secured by encryption or a protected distribution system. Fiber optic lines can be adequately protected by Intrusion Detection Optical Communications systems approved by NSA and listed in the

NSA Information Systems Security Products and Services Catalogue.

c. Protection

(1) Information The security safeguards applied to SBU information during transmission will be consistent with the need for protection against disclosure, loss, misuse, alteration, destruction, or non-availability of data.

(2) Sensitive but Unclassified information as described in AR25-IA shall be protected in transmission by an NSA approved technique unless a waiver is granted under procedures established by DISC4.

(3) NSA-approved techniques, which may be used separately or in various combinations, to protect the transmission of SBU, are listed below:

(a) Encryption. A number of cryptographic products are acceptable for this purpose and are listed in NSA Information Systems Security Products and Services Catalogue.

(1) Type I products. These products may be used to protect both classified and SBU defense information.

(2) Type II products. These products may be used to protect only SBU information; they are handled as an Endorsed for Unclassified Cryptographic Item (EUCI). A FORTEZZA card is an exception to this policy when used in "FORTEZZA for classified applications."

(3) Data Encryption Standard (DES) Equipment. Unclassified cryptographic equipment employing the DES algorithm, which meets the requirements of Federal Standard 1027, may be used to protect only the transmission of unclassified information.

(4) Commercial Equipment. As other equipment is developed and available, when approved by NSA (for example, Rivest, Shamir and Adleman Public Key Encryption System (RSA)), it can be used to protect SBU information.

(b) Unencrypted cable circuits. Although encryption is the preferred protection, unencrypted cable circuits of copper or fiber optics may be used. The degree of protection provided will depend on the type of cable used. The cable least vulnerable to exploitation is fiber optic cable, followed by copper coaxial cable and copper strand cable. Unencrypted cable circuits can be employed to transmit SBU information under the following two conditions:

(1) The cables are used only within the geographic boundaries of the United States or within areas totally within U.S. control overseas.

(2) Adequate measures are implemented such that circuits are maintained on cable and not converted to unencrypted radio transmission.

(c) Protected services. Commercial telecommunications companies offer services that are endorsed to protect the transmission of unclassified information. The companies authorized to offer such services are listed in NSA Information Systems Security Products and Services Catalogue.

(d) A Secure Telephone Unit, Generation III (STU-III) or a Secure Telephone Equipment (STE) may be used to transmit classified data to another STU-III or STE. Both must be keyed to the highest level of information to be passed (i.e., to pass SECRET data, both STU-III or STE must be keyed to the secure SECRET level). The vulnerability exists that higher level information could inadvertently be passed between the STU-III or STE because there are no checks to determine the classification of data. The operators/users must be aware of this vulnerability and ensure that the data transmitted is classified no higher than what the STU-III or STE are keyed to transmit and receive.

(e) Systems connected via STU-III or STE must be accredited at the highest level of classification of information to be transmitted. If the personal computers (PC)

are currently accredited as stand-alone, the systems will require re-accreditation to address communications security. Prior to transmitting classified information to another PC, accreditation statements must be provided to the various participants.

2-26. **Email Security.** Unclassified e-mail system shall be used only for transmission and receipt of unclassified communications. Employees will not transmit classified information over any communication system unless it is transmitted using approved security procedures and practices (i.e., encryption, secure networks, secure workstations).

a. Email threats to the Network:

(1) Denial of Service (e.g. Electronic Chain Letters). Mail-bombing is an email-based attack. The attacked system is flooded with email until it fails. A system will fail in different ways, depending on the type of server and how it is configured. Some Internet service providers (ISPs) give temporary accounts to anyone who signs up for a trial subscription, and those accounts can be used to launch email attacks.

(2) Malicious Codes (viruses, worms, trojan horses) An attacker can attach files to email messages that contain trojan horse executables, virus-infected files or documents that can contain potentially dangerous macros.

(3) Impersonation/Masquerading. The originator of an email message cannot always be trusted. The originator can create a false return address, modify the header in transit, or can connect directly to the SMTP port on the target machine. Digital signatures can be used to authenticate the originator of a message and to protect the integrity of its contents. A digital signature is a string of digits produced by cryptographic algorithms that is transmitted with the message.

Digital signature methods generally use a one-way hash or message digest algorithm to detect changes in the contents of a message, and a cryptographic algorithm to protect the hash.

(4) Eavesdropping. Email headers and contents are transmitted in the clear. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message. Eavesdropping can be prevented by encrypting the contents of the message or the channel over which it is transmitted.

(5) Junk and Harassing Email. Anyone in the world can send you email, it can be difficult to stop someone from sending it to you. People can get your address from company email directories, subscriber lists, or USENET postings. If you give your email address to any Web site, they can resell your address to junk mailers. Some Web browsers volunteer your email address when you visit a Web site. A possible solution is to block this type of email through use of filters or rules if available on your system.

b. Essential steps to secure your e-mail system:

(1) (1) Promote security awareness

(2) Use encryption

(3) Ensure the physical security of the mail server

(4) Ensure antiviral software is installed and properly configured on email servers and client workstations.

(5) Do not share individual email accounts or passwords

(6) Email password should differ from the network password

(7) Users should be warned to treat unusual email messages the same way they treat unusual parcels, with caution.

(8) Use of digital signatures to authenticate a message

c. Internet Electronic Mail protocols are:

(1) Simple Mail Transport Protocol (SMTP) - a host-to-host email protocol

(2) Post Office Protocol (POP) - the most popular email retrieval protocol. A POP server allows a POP client to download email that has been received via another email server

(3) Internet Mail Access Protocol (IMAP) - a newer and less popular email retrieval protocol. IMAP is more convenient for reading email while traveling than POP, since the messages can be left on the server, without having to keep the local list and server list of read email messages in sync.

(4) The most common Internet email transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing email messages to be easily forged. Nor do these protocols require the use of encryption, which could ensure the privacy of email messages. Although extensions to these basic protocols exist, the decision to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that is supported by both ends. If you must use POP or IMAP, ensure you use secure socket layer (SSL).

(5) Multipurpose Internet Mail Extensions (MIME) redefines the format of email messages. It can be used to support security features like digital signatures and encrypted messages. MIME has been used to mail virus- infected executables and dangerous messages and attachments. Install and configure antiviral software to scan and remove malicious code from attachments.

(g) Commercial Internet Service Providers (ISP). To support mission requirements, access to the Internet is generally made via Army or DOD owned gateways. Army organizations may use commercial ISPs as required by the local architecture, security environment or other factors. See AR 25-1 for further guidance.

2-27. Internet, Intranet and WWW Security.

a. Access - Many unclassified Army systems provide access to the internet. The Army promotes the use of the Internet but appropriate safeguards must be established to prevent and detect technical attacks made on Army systems and to ensure classified or sensitive information is not inadvertently released to unauthorized personnel. Use of the internet, from government owned or leased computers is limited to unclassified, official government business, and those authorized purposes as set forth in DOD 5500.7, Joint Ethics Regulation, the Standards of Ethical Conduct, 5 CFR 2635.704, and AR 25-IA. The Joint Ethics Regulation allows users limited use of DOD telephones, E-mail systems, and Internet connections for personal use, so long as such uses are on a not-to-interfere basis and are not for an improper purpose such as conducting a private business.

(1) Before the user is authorized access to the Internet, the user must have received ISS awareness training, and be issued an account and password.

(2) Personnel will not share email and internet accounts with other personnel. However, MACOMs may establish group email/group accounts as a cost-saving measure. A list of users who may access the group account must be maintained. The individual user is responsible for all activity during access to the account.

(3) Users are not to use private accounts for Army-related business unless specifically authorized to do so by their Director of Information Management/Deputy Chief of Staff for Information Management (DOIM/DCSIM).

(4) Users are authorized to download and upload programs, graphics, and textual information from the Internet to an

unclassified Government-owned personal computer as long as it does not violate federal and state law, regulations and local policies.

(5) Personnel will scan all files for viruses before storing, transmitting, or processing information within Army computers, systems, or networks.

(6) Government-owned or leased personal computers will not be used to access commercial services such as CompuServe, America on Line, or Prodigy, unless a government-acquired subscription to such services is in place and the access is for official business only.

(7) Access to the Internet can be controlled through the use of software which blocks objectionable web site categories as determined by the DAA. Examples of blocked categories are criminal skills, drugs, extreme or obscene, gambling, and sex).

(8) Appropriate access and security controls (fire walls, restriction by IP address, etc.) must be used to ensure data integrity. If the account is accessed via a local area network, a combination of access and security controls must be in place. If the connection is made via a modem, the computer must be logged on to a valid authentication server, such as Terminal Server Access Control System (TSACS), or operate in a standalone mode.

(9) No classified or Sensitive But Unclassified (SBU) information, will be placed on any publicly accessible server.

(10) No classified information will be placed on any unclassified Intranet servers. at any time.

(11) SBU material should not be hosted on an Intranet server unless specific security features appropriate to the level of the SBU data are implemented. For Official Use Only (FOUO) and SBU information that is hosted on an Intranet server must be protected and approved by the appropriate DAA. Material provided on Intranets that is SBU or FOUO will not be made available to the public at large without the written approval from the organizations Commander or DAA.

(12) Extranet information will be provided using selected intranet servers which are connected to external users via devices which provide adequate encryption and user authentication.

(13) All information systems with servers (including web servers) which are connected to unclassified publicly accessible computer networks such as the internet, will employ a combination of access and security controls (firewalls, routers, etc.) to ensure the integrity, confidentiality and availability of DOD information systems and data. The user will not attempt to "talk around" classified topics while communicating on the Internet, including e-mail. Personnel shall only conduct classified discussions on systems approved for the appropriate classification level, i.e., SIPRNET, and JWICS.

b. Home pages and web sites. Public accessible web sites shall be on a server in the DMZ as defined in the NSIP. Army web sites provide value added information services and products through the sharing of accurate, timely, and relevant information. Home pages and web sites may be created allowing access to the public at large or to a limited audience. The links to information on web sites intended for limited audiences should have access controls. These controls should be administered by the web-master or system administrator. Web-masters or systems administrators shall develop and publish local policies for the submission of information onto the organization's home page. Publishing Army information onto electronic bulletin boards or WWW home pages constitutes the public release of information and must comply with the established policy for the release of specific information. Personnel wishing to release Army information must first ensure that they have public release authority. Clearance of specific information shall be directed to the

appropriate proponent, the local public affairs office, or foreign disclosure office. Display of classified information, For Official Use Only information, DoD contractor proprietary information, information that violates operations security, and Freedom of Information Act exempt information for which the agency declines to make a discretionary disclosure are prohibited. Privacy Act information is protected. Do not place information that has value to only military or other government agencies on Internet pages with unlimited access. Consider using an Intranet, instead of Internet, connection for dissemination of this type of information. Home page and organizational web pages use information provided by functional proponents (users). Functional proponents are responsible for:

(1) Information content on Web pages,

(2) Keeping information current, and accurate,

(3) Home Pages and Web Site information will not contain personal or Privacy Act Information (such as family member names, personal photos and addresses, home phone numbers, career history, resumes, previous assignments, awards, or schooling). Information that extends beyond the duties and responsibilities of the person's organization, commercial advertising, and product endorsement is prohibited. Staff sections and subordinate command Commanders are responsible for assigning Webmasters for their respective web pages.

(4) Intranet Webmasters will:

(a) Be responsible for the information content on their web sites.

(b) Keep information on web pages current, and accurate.

(c) Obtain approval from the DAA prior to implementing an Intranet web site.

(d) Maintain linkages with all approved Intranet Home Pages. Hyperlinks from Internet sites to Intranet sites are prohibited.

c. Reporting suspicious activity - Army Internet, Intranet, and Extranet sites are considered as lucrative intelligence sources and are targeted for information collection efforts. Army personnel must report suspicious activity to the appropriate IA personnel. The Copyright Act, the Freedom of Information Act, the Privacy Act, and statutory Federal records requirements also contain provisions with which users must comply. Users should consult these guidelines and the office of the local staff judge advocate regarding any Internet activity that raises legal concerns.

d. Requests for information The MACOMs are responsible for any search and review of their holdings of Internet data, for purposes of responding to requests for information pursuant to the Freedom of Information Act, the Privacy Act, congressional or other investigative inquiry. All official contacts with the media must be made through the appropriate Public Affairs Office.

e. DAA approval - The Designated Approving Authority (DAA) approval is required before connecting any system to the Internet. Under no circumstances will users permit dial-in access to their computer via the individual modem, without specific written permission from the DAA.

f. Use of cryptography, authentication techniques, and incident response activities are available to improve security on the Internet.

2-28. AB SWITCHES. AB switches are switchboxes that allow a user the capability to share hardware peripherals. An AB switchbox will allow a user to share one console between two workstations or PC's or two monitors for one workstation or PC. DIA/DAC-2 approves the use of the black box server switch, models SW721A-R2 and SW723A-R2 (consistent with physical and AIS security accreditation) for collateral and SCI systems within DIA SCIFS provided the following restrictions are met:

(1) No smart mouse or smart keyboards can be used (no or limited buffering capability restricted to only what is needed for the equipment's operation functions).

(2) Disk drive must be conspicuously labeled, with a clear and immediately recognizable label that identifies the classification level of workstation/system it connects to.

(3) When in use the monitor must display the classification level of workstation/system that it is connected to.

(4) Written standard operational procedures must be provided to each user of workstations/systems that utilize the black box server switch, model SW721A-R2 or SW722-R2. It must outline the configuration, activation, and operation procedires for the collateral and SCI modes of operations.

(5) As a minimum for red/black separation guidance all equipment and cables should be installed using the NSTISSAM Tempest/2-95, DTD 12 Dec 95, Red/Black Installation, section 3 and the appropriate recommendation as specified by the inspectable space determination for each SCI facility. Separation distances for wire lines are based upon the wire lines having one overall shield.

(6) DIA/DAC-2A must be advised when and where the black box server switch, models SW721A-R2 and SW722-R2 are installed. See DIA IAW message DTG 291804 OCT 98, Subject: Tempest Evaluation of the Black Box Server switch models SW721A-R2, SW72A-R2, and SW722A-R3 (U), 690 ISS, Fax, DTD 21 Oct 98, Black Box Server switch Evaluation Documentation (U), and NSTISSAM Tempest /2-95, DTD 12 Dec 95, Red/Black Installation .

2-29. Internetworking Security Tools.

a. Configuration Management. Configuration Management shall be used to ensure that development and changes to an Information System (IS) takes place in an identifiable and controlled manner.

(1) The following three specific aspects of configuration management are used to provide assurance that modifications to the network environment do not adversely affect the security of the system

(a) Identification. Configuration identification employs the identification of system components and documentation that supports security control procedures. The following criteria establishes a baseline to be used for configuration identification:

?? Identify major equipment components (make, model and serial number) of CPU, plotter, printer, scanner and other peripherals.

?? Equipment configuration (identify fixed hard drives, removable hard drives, read/recordable compact disk drives, Personal Computer Memory Card International Association (PCMCIA) cards, multimedia, internal fax/modem, external modem, switch devices).

?? Identify software by type, title and version.

?? Identify patches, upgrades and hot fixes

?? Validate Y2K compliance

(b) Configuration controls. Configuration controls are performed by subjecting system components and documentation to a review and approval process within the organization. Configuration control is implemented by modification controls.

(c) Modification Controls. Modification controls identify the procedures used to evaluate, coordinate, and submit for approval requests for IS modifications. System modifications shall be coordinated with the appropriate IA personnel at the earliest opportunity. The modification shall be analyzed to determine the expected impact on security caused by the changes.

(2) Only essential network services shall be enabled. Turn off as many services and applications as possible, and selectively enable those that are essential.

(3) All default passwords shall be changed.

b. Audit files. IS configuration auditing. The appropriate IA personnel shall be responsible for a continual auditing program, which assures proper IS configuration identification. Test systems to confirm configurations.

(1) Audit Files shall be reviewed.

(2) The responsible IA personnel shall perform system audits to verify secure operation of the system and support software. If irregularities are discovered, begin an analysis to identify the problem (exploring all possible alternatives) and corrective actions necessary to resolve the situation. The responsible IA personnel maintain historical records of audit problems and corrective actions.

c. Information Assurance Tools

(1) Only the use of DISC4 approved IA tools are authorized to periodically review network security. The approved IA tools are available through the ACERT web site. Some network management software packages contain utilities, which are similar to those in the IA tool set. These tools may be used to map the network and to conduct automated scans of individual machines for configuration errors that could lead to unauthorized access to individual machines and/or the network. At no time will the IA tools or network management software tools be used to review user data even though the tool is capable of this function.

(2) IA personnel are not authorized to use hacker techniques in an attempt to penetrate an AIS. Such penetration testing will be authorized only in accordance with AR 380-53. Techniques include but are not limited to:

(a) The use of network analyzers, sniffers, or similar network monitoring systems to monitor the activities of specific system users. The use of these devices is authorized to perform valid system troubleshooting and diagnostics of network problems.

(b) "Keystroke monitoring" software of any kind will not be used either resident on the user's computer, or by monitoring computer network communications.

(c) The use of keyboarding or automated techniques to exploit/verify vulnerabilities identified by the Information Assurance.

d. Internetworking Devices. Other tools employed by the Army:

(1) Intrusion Detection System (IDS). ASC in coordination with DISC4 and the ACERT currently operate an IDS device for every Army activity connected to the NIPRNET. The IDS operates on a Unix and NT platform and utilizes a commercial off the shelf (COTS) software package known as RealSecure. This package provides the means of examining packets of information in transit looking for known attack signatures. These systems are constantly monitored by either the ACERT or it's Regional Computer Emergency Response Teams (RCERT). Although ASC owns, operates, and maintains the IDS device, this does not preclude the appropriate activity IA personnel from monitoring and analyzing the data. Local monitoring of the IDS may be done with approval of the appropriate RCERT. The request should document the operational requirement, the intent of monitoring, and the impact if not approved. The request will be staffed through the Information Assurance Manager (IAM) or the equivalent, and submitted to the applicable RCERT (or directly to the ACERT for those in the National Capital Region (NCR)). If approval is granted, the requesting activity is responsible for providing the hardware and obtaining a copy of the RealSecure software. Configuration of software will be coordinated with the appropriate RCERT.

(2) The Internet Scanner is another COTS application developed by Internet Security Systems as part of the RealSecure suite of products. The scanner is one of the available

products used by the ACERT and the RCERT to scan Army networks and detect vulnerabilities.

(a) Internet Scanners shall only be used by a trained and certified individual. LIWA has established a Vulnerability Assessment Certification (VAC) program, which upon successful completion provides the proper level of certification to conduct scanning and/or mapping of a network. Another level of certification is required for those individuals responsible for analyzing the resulting data.

(b) Prior to conducting this type of mapping/scanning of a network, the activity IAM must inform the ACERT or appropriate RCERT of their intent to perform a scan. A reason for this coordination is that the Internet Scanner employs some techniques, which give the appearance of a network attack. All scans shall be formally documented and subject to later review by the ACERT or appropriate RCERT. Documentation shall include as a minimum:

Name of person requesting scan/assessment

Name of approving official

Intent (reason for scan)

Scope (full network, subnet, segment)

Methodology (High/Medium/Low risk)

Date & time scan conducted

Date & time complete

Name, organization, and phone number of individual conducting scan

Date, level, and method of certification

Date, time, name of ACERT (RCERT) POC with whom this action was pre-coordinated.

Copy of findings

(c) Installations that do not have the expertise, requisite level of certification, or resources to scan their own networks, may request a vulnerability scan through the ACERT (see sections titled: Vulnerability Assessment & CDAP).

(d) Unauthorized scans of networks will be treated as intrusions and reported to the ACERT upon detection. Persons conducting unauthorized scans of Army networks may be subject to adverse actions or UCMJ.

CHAPTER 2, SECTION IX, & X: IS REPORTING, TACTICAL SECURITY (DEVELOPED BY COMMITTEE # 5)

SECTION IX

IS INCIDENT REPORTING

2-30. Definitions:

a. IS Security Incident—Any unexplained event that could result in the loss, corruption, and/or the denial of access to data, as well as any event that cannot be easily dismissed or explained as normal operations of the system.

b. IS Serious Incident – Any event that poses grave danger to the Army's ability to conduct established information operations.

2-31. Types of Incidents

a. Examples of the types of security incidents that will be reported include but are not limited to the following:

(1) Known or suspected intrusions or attempted intrusions into classified and unclassified AIS by unauthorized users or by authorized users attempting unauthorized access

(2) Unauthorized access to data, files, or menus by otherwise authorized users

(3) Indications of an unauthorized user attempting to access the AIS, including unexplained attempts to log-on unsuccessfully from a remote terminal

(4) Indications of unexplained modifications of files or unrequested “writes” to media

(5) Unexplained output received at a terminal, such as receipt of unrequested information

(6) Receipt of inappropriately classified output, such as classified data received on an SBU system

(7) Inconsistent or incomplete security markings on output with extraneous data included in the output, or failure to protect the output properly

(8) Abnormal system response

(9) Malicious code, such as virus, trojan horse, applet, macro virus

(10) Alerts by network intrusion detection systems (IDS) installed to detect “hackers” and other unauthorized personnel attempting system penetration

(11) Entries in audit/system logs (including but not limited to those found on servers, workstations, firewalls, intrusion detection systems (IDS), routers, and switches) indicating unauthorized access or misuse of information systems.

b. Examples of IS Serious incidents include but are not limited to the following, which were extracted from the Department of Defense (DOD) Information Operations Condition (INFOCON):

(1) Indications and warnings (I&W) denoting the targeting of specific system, location, unit, military operation or contingency, planned/ongoing.

(2) Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance.

(3) Network penetration or denial of service attempted with major impact to military operations.

(4) IS attack(s) detected with major impact to military operations

(a) Widespread incidents that undermine ability to function effectively.

(b) Significant risk of mission failure.

2-32. Classification Guidance

a. Classified and Sensitive but Unclassified (SBU) incident reports will be protected by encryption or a protected distribution system (PDS) during transmission. Refer to Sections 4-2 and 4-3 [CHECK PARAGRAPH NUMBERS WHEN DA PAM COMPLETED] of this DA PAM for encryption and PDS requirements.

b. At a minimum SBU reports will be marked and handled as For Official Use Only (FOUO) and are exempt from release under the Freedom of Information Act and The Privacy Act of 1974 IAW AR 25-55 AND AR 340-21.

c. Classification guidance

d. A serious incident that would cause a commander to raise the INFOCON level to BRAVO or higher will be classified, at a minimum at the SECRET level. The classification will be commensurate with the system high watermark (SHWM) of the affected system/network.

e. The following list includes additional classification requirements as documented in the Army Digitization Office, Digitization Security Classification Guide:

(1) Incidents that include a specific Internet Protocol (IP) address that points to a classified host will be marked and handled as Secret for a period of 10 years

(2) Unauthorized intrusions if:

(a) Suspected or determined to be hostile intrusion will be marked and handled, as a minimum, Confidential for a period of 10 years

(b) A benign intrusion (unauthorized insider, tester, or official evaluation) and the specifics of how the intrusion occurred are not provided will be marked and handled as FOUO

(3) Specific vulnerabilities of an individual critical C4I system that would aid its being defeated by an adversary will be marked and handled Secret for a period of 10 years.

(4) Incidents that include detailed security device configuration data (firewall setup parameters, INE data bases, etc) will be marked and handled, as a minimum, confidential for a period of 10 years

2-33. Reporting Structure.

a. The following checklist defines incident responsibilities for personnel involved in the use of an IS and the IA Incident Reporting Structure.

b. All incidents will be reported in the following manner:

(1) The USER will:

(a) Inform the Systems Administrator (SA) of the potential incident by the quickest means possible.

(2) The SYSTEM ADMINISTRATOR will:

(a) Make a determination if the event is reportable as an IS Incident as defined in this DA PAM.

(b) Obtain enough information to complete an Initial Incident Report (Figure XX)

(c) Forwarding that report to both the Information Assurance Security Officer (IASO) and the Information Assurance Network Officer (IANO)

(d) Forward the report NLT X hour after receiving initial information or discovering the incident themselves.

(e) Create and forward the report to both the IASO and IANO for any incident detected as part of normal duties, such as those identified by but not limited to IDS, C2 Protect Tools, and audit logs.

(3) The IASO will:

(a) Determine the incident severity and impact on the IS [MARKER – add severity criteria]

(b) Inform their immediate chain of command

(c) Forward the report to the IAM.

(d) Determine if the incident meets the criteria outlined in this DA PAM concerning Serious Incidents,

(e) Prepare a Serious Incident Report SIR) IAW AR 190-40, if it is determined that it is a serious incident. The SIR is an additional requirement and does not replace the normal reporting requirements.

(f) Contact the Counterintelligence (CI) element with jurisdiction, if espionage or sabotage is suspected.

(g) Contact the Criminal Investigation Division (CID) unit with jurisdiction, if criminal activity is suspected.

(4) The IANM/IANO will:

(a) Determine the incident severity and impact on the network of any incident reports received from the SA

(b) Initiate corrective action

(c) Create a report for any incident detected as part of normal duties, such as those identified by but not limited to IDS, C2 Protect Tools, and audit logs

(d) Forward the report to the IAM

(e) Forward the report NLT X hour after receiving initial information or discovering the incident themselves

(f) Determine if the incident meets the criteria outlined in this DA PAM concerning Serious Incidents

(g) Prepare a Serious Incident Report SIR) IAW AR 190-40, if it is determined that it is a serious incident. The SIR is an additional requirement and does not replace the normal reporting requirements.

(5) The IAM will:

(a) Validate the severity of the incident

(b) Forward to the RCERT for action and the Network Operations Center (NOC), MACOM IAPM and MACOM IANM for information.

(6) The MACOM IAPM and MACOM IANM will:

(a) Consolidate incident reports for their MACOM

(b) Provide to MACOM Commanders

(7) Tenant Activity(s):

(a) Will follow the process identified above

(b) IANM/IANO will Furnish reports to the host installation IANM/IANO and IAM

(8) The NOCs will:

(a) Create a report for any incident detected as part of normal duties, such as those identified by but not limited to IDS, C2 Protect Tools, and audit logs.

(b) Forward to the appropriate RCERT

(9) The RCERT will:

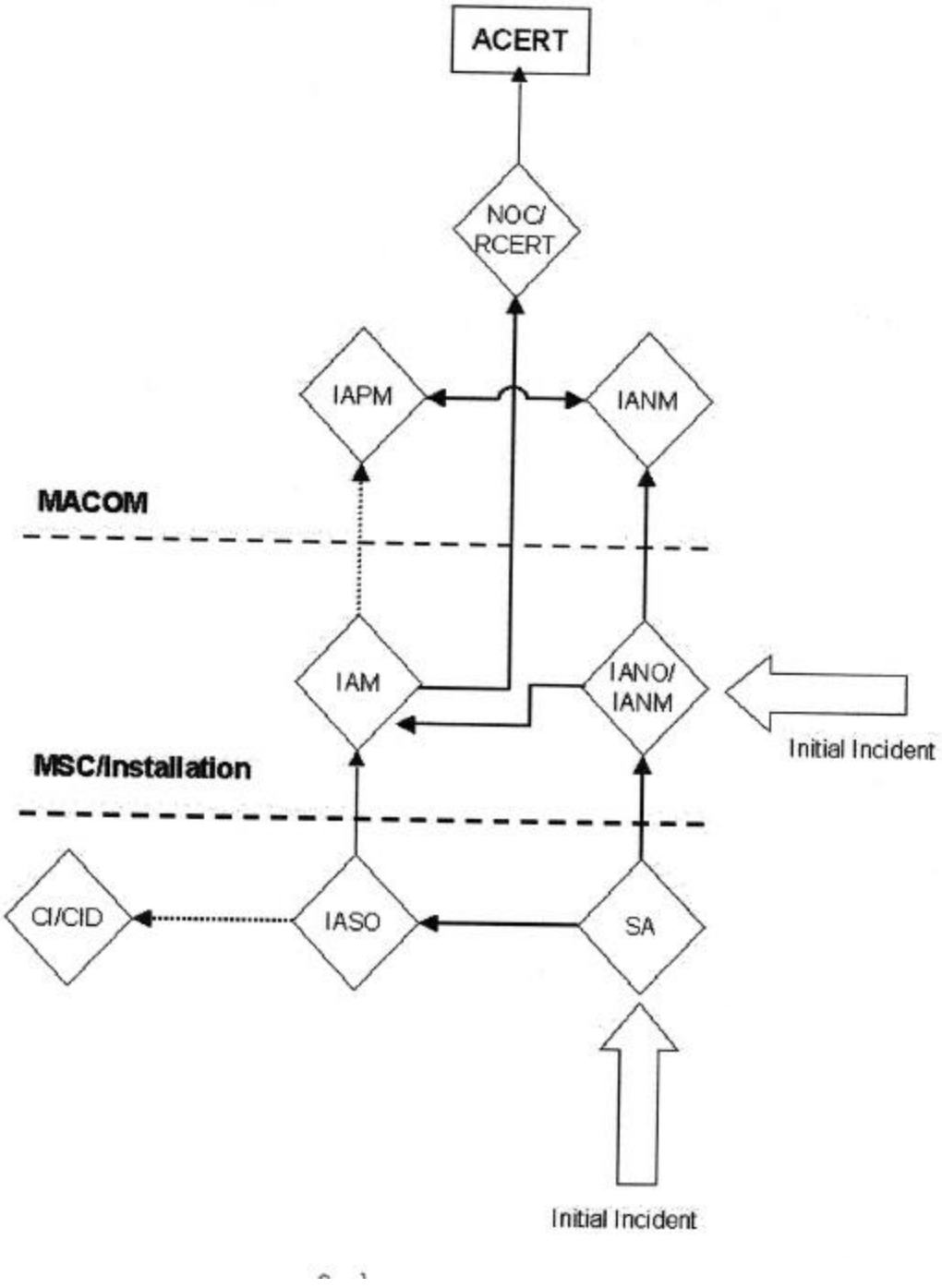
(a) Furnish reports to the ACERT/CC and the other RCERTs

c. When information is discovered at a higher classification than the SHWM (for example, Secret information on systems operating at the SBU level, TS information on systems operating at the Secret level) the incident will be reported to the Security Manager IAW AR 380-5. This is an additional reporting requirement that applies to everyone, and does not replace the normal reporting requirements.

d. IAW AR 25-IA, SAs, Network Administrators and personnel in the IA Incident Reporting structure are not authorized to provide further investigative support, other than providing information concerning actions taken as a result of the initial report, to law enforcement and intelligence agencies unless the representative from the investigative agency can provide proof that there is an official investigation open. Personnel should review AR25-IA and or seek legal advise from the Staff Judge Advocate prior to providing support to investigative personnel to ensure that they do not violate any provisions of the regulation.

d. Reporting of computer incidents will be through the established IS Incident Reporting Structure shown in Figure 1. If this cannot be accomplished in a manner that would prevent further damage, misuse, unauthorized access, denial of service of critical IS or without risking the safety of personnel, then the incident should be reported directly to the first available person in the IA chain, to include directly to the ACERT 1-888-123-1234. At the earliest possible moment reports will be submitted IAW the IS Incident Reporting Structure. This DA PAM does not prohibit directly reporting a computer event or incident to any official that may provide assistance.

FIGURE 2-31A


ACERT
NOC/
RCERT
IAPM
IANM
MACOM
IAM
IANO/
IANM
Initial Incident
MSC/Installation
CI/CID
IASO
SA
Initial Incident

2-34. Timeline for Reporting IS Incidents

Potential incidents will be reported immediately upon recognition. The incident report will be generated as previously described in paragraph 1.4 and travel through the IS Reporting Structure to the ACERT (Figure(1) within 24 hours IAW ACERT instructions.

2-35. Verification and Validation (V&V) of Reporting ProcessProcedures for reporting and investigating security incidents should be developed and tested before the systems/network becomes operational IAW AR 25-IA.

2-36. IS Incident Report Format

a. The following form will be completed to the extent possible in reporting incidents other than virus incidents in environments other than tactical.

[CLASSIFICATION]

IS Incident Report Form

1. General Information: Date of Report
   - Incident Number:
     - Installation
     - Unit
     - Address/Bldg Number
     - Domain Name
     - Brief description of organization
   - Contact Information
     - Name/Rank
     - Job Title
     - Email address
     - Telephone number (COMM/DSN)
   - Telephone Number STU III
     - Unclassified FAX number
     - Classified FX number
     - Pager number
   - Contact information for any other incident response teams that have been notified
     - Name
     - Team/Organization
     - Title
     - Telephone number
     - Tracking number
   - Contact information for any law enforcement or counterintelligence agencies notified
     - Agency/Unit name
     - Contact person name
     - Telephone number
     - Incident reference number

2. Host Information (Please provide information all hosts involved in this incident at the time of the incident):
   - Host name
   - IP Address
   - Classification of host
   - Timezone of the involved host
   - Vendor hardware
   - Operating System(s) and version(s)

3. Function of involved host(s)
   - Router
   - Terminal Server
   - Mail Server
   - DNS Server
   - WWW Server
   - FTP Server
   - Database Server
   - Other (describe)
   - What mission does this host support (describe)

What function is this host responsible for (describe)

Was this host compromised as a result of this attack?

4. What impact did this incident have on the host's ability to complete its mission?

5. Incident Categories (Please mark as many categories as are appropriate to this incident)
   - Probe/scan
   - Email bombardment
   - Anonymous FTP abuse
   - Break-in
     - Intruder gained root access (Yes/No)
     - Intruder installed Trojan Horse program(s) (Y/N)
     - Intruder installed packet sniffer (Y/N)
       - What was the full path name of the sniffer output files
       - How many sessions did the sniffer log?
   - NIS (yellow pages) attack (Y/N)
   - NFS attack (Y/N)
   - TFTP attack (Y/N)
   - FTP attack (Y/N)
   - Telnet attack (Y/N)
   - Rlogin or rsh attack (Y/N)
   - Cracked password (Y/N)
   - Easily guessable password
   - Web Server
     - Phf vulnerability probe
     - Nph-test-cgi probe
     - Other
   - IP spoofing
   - Product vulnerability (specify)
   - Configuration error
   - Default Accounts
   - Misuse of host resources (describe)
   - Other (please specify)

6. Security Tools (At the time of the incident, were you using the following security tools):
   - Network Monitoring Tools
     - NID
     - ASIM
     - JIDS
     - Misc Network Analyzer
   - Authentication/Password tools
     - Crack
     - Shadow passwords
     - One time passwords
   - Service filtering tools
     - Host access control via modified daemons or wrappers
     - Firewall (what product)
     - TCP access control using packet filtering
   - Tools to scan hosts for known vulnerabilities
     - ISS
     - SATAN

Multi-purpose tools
- SPI
- COPS

File Integrity Checking Tools
- MD5
- Tripwire

Other tools

lsof (list open files)
- cpm
- smrsh
- Append-only file system

Additional tools (please specify)

7. Detailed description of the incident

Date and duration of incident

How you discovered the incident

Method used to gain access to the affected host(s)

Details of vulnerabilities exploited that are not addressed in previous sections

Other aspects of the attack

Hidden files/directories

The source of the attack (if known)

Steps taken to address the incident (e.g., binaries reinstalled, patches applied)

Do you plan to start using any of the tools listed above in question 5.0 (please list tools expected to use)

Other

8. Please append any log information or directory listings and timezones information (relative to GMT)

Syslog
Utmp
Wtmp
TCP wrapper
Process accounting

What do you believe the reliability and integrity of these logs (e.g., are the logs stored offline or on a different hosts)

9. Please indicate if any of the following were left on your system by the intruder
   Intruder tool output (such as packet sniffer output logs)
   Tools/scripts to exploit vulnerabilities
   Source code programs (such as Trojan horse programs, sniffer programs)
   Binary source programs (such as Trojan horse programs, sniffer programs)
   Other files

10. If you answered yes to any of the last five questions, please call the ASSIST hotline (1-800-XXX-XXXX) for instructions on uploading files by FTP

11. What assistance would you like from the ASSIST?

THIS DOCUMENT IS EXEMPT FROM THE DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT X, X [NEED CORRECT REFERENCE]

b. The following form will be used to report virus incidents.

Virus Reporting Form

1. Personal Information
   NAME
   PHONE (COMM) DSN
   Email Address
   Location (Installation, Bldg, Room)

2. Virus Information
   Name of Virus (if known)
   Anti-Virus Used (McAffee, Norton or name of other)
   Date/Time/Time Zone Incident Occurred
   Date/Time/Time Zone Incident Reported
   Date Cleaned

3. Computer Information
   Number of Systems Infected
   Operating System(s) Infected

System(s) IP Address
Classification of Computer(s)

4. Damage Report
   Mission of computer
   Impact of virus on mission
   Damage/Observation

5. Source of Infection
   Email (source name if known)
   HTTP/WWW (source IP Address or URL if known)
   FTP (source IP Address, directory, file if known)
   Network (NIPRNET, SIPRNET, JWICS, or name of other)
   Floppy (source of floppy)
   Other (explain)

THIS DOCUMENT IS EXEMPT FROM THE DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT X, X

c. The following forms will be used to report IS incidents other than viruses in a tactical environment.

[CLASSIFICATION]

Tactical IS Incident Report

1. Date & Time Incident Observed or Noticed

2. Date & Time Incident Reported

3. Action Taken to Protect System/Network

4. Contact Information
    a. Name/Rank
    b. Job Title
    c. Unit
    d. Location
    e. Email address
    f. Telephone number (COMM/DSN/MSE)

5. Location of Incident
    a. IP address of affected system(s)
    b. Physical location of system(s)
    c. Classification of information processed on system or network
    d. Type device

Router	Terminal Server
Mail Server	DNS Server
WWW Server	FTP Server
Database Server	Stand Alone
Networked workstation/PC	Other (describe)

6. How was this incident detected?

7. What mission does this host support (describe)

8. What function is this host responsible for (describe)

9. Was this host compromised as a result of this incident?

10. What impact did this incident have on the host's ability to complete its mission?

11. Does the computer contain an approved warning banner?

12. What is the impact to the Army of the information lost (if applicable)?

13. What is the current system status? (On-line/Off-line)

14. Is the affected system covered by an IDS? (If Y, Name of IDS(Real Secure, CISCO, etc))

15. Is the affected system covered by a Firewall? (If Y, Name of Firewall (Raptor, CISCO, etc))

16. Describe Incident:

THIS DOCUMENT IS EXEMPT FROM THE DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT X, X

SECTION X

TACTICAL SECURITY

2-37. Tactical Security.

a. This section applies to automated tactical systems (ATS) and automated weapon systems (AWS).

An automated tactical system is any AIS that is used for communications, operations, or as a weapon during mobilization, deployment or tactical exercises. An ATS may include but is not limited to data processors, firmware, hardware, peripherals, software or other interconnected components and devices such as radar equipment, global positioning devices, sensors, guidance systems airborne platforms. An automated weapon system utilizes a combination of computer hardware and software, which performs the functions of an automated information system such as collecting, processing, transmitting, and displaying information, in its operation. ATS and AWS will implement the requirements of AR 25-IA and this DA Pam with the exceptions listed in this section. When deployed either in field exercises or real world operations the following criteria apply.

b. Passwords. Passwords on ATS and AWS may be shared based on need-to-know when failure to do so would result in loss of life or mission failure.

c. User lockout. The system will not create a denial of service that would impede mission success through user lockout. For example, user lockout resulting from inactivity time period, unsuccessful logon attempts, automated screen saver features, and aged passwords.

d. An automated alert will be generated by the system and sent to the SA as a result of three unsuccessful logon attempts.

e. E-Mail

(1) Private e-mail accounts, e.g., AOL, MSN, will not be authorized for use in tactical systems

(2) Unauthorized external connections will not be introduced for the timely use of e-mail

(3) Unauthorized e-mail software will not be loaded/used on tactical information systems

(4) Only e-mail services deemed to be mission essential and approved by the DAA will be used on tactical systems

f. World Wide Web (WWW)

(1) Java, java script, cookies

(2) Only WWW services/accesses deemed to be mission essential and approved by the DAA will be used on tactical systems

g. External Connections

(1) Communication/connections outside the tactical network will not be introduced without the specific approval of the DAA

(2) The DAA must consider the impact on the overall network risk level when allowing additional connections to the tactical network

h. Telecommunications Devices

(1) Privately owned receiving, transmitting, recording, amplification, and processing equipment, are not to be used or permitted within the confines of any area designated by the commander to be a classified work area, restricted area, Mission Essential Vulnerable area, staging area prior to deployment, or deployment.

(2) Government owned receiving, transmitting, recording and amplification equipment, and or other non-secure telecommunications equipment are not to be used unless declared in writing by the local commander as mission essential prior

to use in areas designated to be a classified work area, restricted area, Mission Essential Vulnerable area, staging area prior to deployment, or deployment.

i. Maintenance. Uncleared, untrained or foreign national personnel will not perform maintenance on any weapons systems. Any weapon system that does not include automated capabilities (for example, M16, 81MM mortar system) is excluded from this requirement.

j. Network Classification Level. All systems including the tactical network will operate at the same SHWM, for example, unclassified information, unclassified media, uncleared users, network SHWM is Unclassified.

k. Foreign nationals –

l. Imminent Capture. Mechanisms will be available and used to render the Tactical system inoperable in case of imminent capture.

m. IS Incident Reporting. The IS reporting structure is the same for both tactical and non-tactical systems with the following exceptions.

(1) Timelines. Users will report potential incidents immediately to the SA. Incident reports will move through the IS Incident Reporting Structure, SA to RCERT, in no longer than 4 hours. The incident report will move from the SA to the IANO and IASO within one hour for action. Upon receipt of the incident report the IANO and IASO will immediately forward to the IAM. The IANO and IAM to take the necessary action to protect the network, analyze the situation, inform the commander, and forward to the RCERT in no longer than 3 hours time.

(2) Forms: The following forms will be used to report incidents and viruses in the tactical environment.

[CLASSIFICATION]

Tactical IS Incident Report

1. Date & Time Incident Observed or Noticed

2. Date & Time Incident Reported

3. Action Taken to Protect System/Network

4. Contact Information
    a. Name/Rank
    b. Job Title
    c. Unit
    d. Location
    e. Email address
    f. Telephone number (COMM/DSN/MSE)

5. Location of Incident
    a. IP address of affected system(s)
    b. Physical location of system(s)
    c. Classification of information processed on system or network
    d. Type device

Router	Terminal Server
Mail Server	DNS Server
WWW Server	FTP Server
Database Server	Stand Alone
Networked workstation/PC	Other (describe)

6. How was this incident detected?

7. What mission does this host support (describe)

8. What function is this host responsible for (describe)

9. Was this host compromised as a result of this incident?

10. What impact did this incident have on the host's ability to complete its mission?

11. Does the computer contain an approved warning banner?

12. What is the impact to the Army of the information lost (if applicable)?

13. What is the current system status? (on-line/off-line)

14. Is the affected system covered by an IDS? (If yes, name of IDS (RealSecure, CISCO, etc.))

15. Is the affected system covered by a Firewall? (If yes, name of Firewall (Raptor, CISCO, etc.))

16. Describe Incident:

THIS DOCUMENT IS EXEMPT FROM THE DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT X, X

VIRUS REPORTING FORM

1. Personal Information

NAME

PHONE: (COMM) (DSN)

Email Address

Location (Installation, Bldg, Room)

2. Virus Information
   - Name of Virus (if known)
   - Anti-Virus Used (McAffee, Norton or name of other)
   - Date/Time/Time Zone Incident Occurred
   - Date/Time/Time Zone Incident Reported
   - Date Cleaned
3. Computer Information
   - Number of Systems Infected
   - Operating System(s) Infected
   - System(s) IP Address
   - Classification of Computer(s)
4. Damage Report
   - Mission of computer
   - Impact of virus on mission
   - Damage/Observation
5. Source of Infection
   - Email (source name if known)
   - HTTP/WWW (source IP Address or URL if known)
   - FTP (source IP Address, directory, file if known)
   - Network (NIPRNET, SIPRNET, JWICS, or name of other)

THIS DOCUMENT IS EXEMPT FROM THE DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT X,X

n. In transit. Commanders will develop policy for the secure transportation and safeguarding of ATS and AWS IAW AR 380-5.

o. Accreditation Responsibilities

(1) Designated Approving Authority (DAA)

(a) A DAA will be appointed for each exercise or deployment.

(b) The DAA is responsible for the exercise/deployment network accreditation and security.

(c) The DAA is the official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk

(2) Certification Agent (CA) for ATS and AWS. The CA for ATS and AWS will be appointed IAW DODI 5200.40, the DITSCAP. If this is not feasible, the CA for ATS and AWS developed under the PEO/PM structure may be the project/product manager.

(a) The CA is responsible for ensuring that the comprehensive evaluation of the technical and non-technical security features of the system and other safeguards are performed in support of the accreditation process.

(b) Individuals who complete the certification process (that is, the certification test plan, certification test, certification report) will be independent from the developer staff

p. Interim Approval to Operate (IATO)

(1) An interim approval to operate is required for all systems, including operational, those in spiral development, and proof-of-concept prototypes, that will be tested, used in exercises or demonstrated prior to completion of an accreditation.

(2) If a test, exercise, or demonstration is a final test prior to a fielding decision; the entire accreditation document in draft format is required.

(3) If a test, exercise, or demonstration is other than a final test before a fielding decision; a Draft Security Plan and a Draft USM/SOP accompanied by an IATO memorandum signed by the DAA is necessary

(4) When a commander chooses to accept a non-fielded system that is not covered by an IATO, that commander becomes responsible for the IATO or operational accreditation of the non-fielded system prior to putting the system into use. non-filed system

CHAPTER 2, SECTION XI, MISCELLANEOUS PROVISIONS (REMOTE DEVICES, LAPTOPS, EMPLOYEE-OWNED, ETC) (DEVELOPED BY COMMITTEE # 3)

2-38. Remote Access

a. Make sure that access tables, when used, remain current.

b. Prohibit the use of call-forwarding capabilities when callback or dialback technology is used.

c. Consider the use of remote access technology, (e.g., dial-in modems) during the risk analysis and the security test and evaluation and document it in the system security policy.

d. Annotate remote access in the audit logs.

e. Do not publicize modem telephone numbers to anyone other than those with a need-to-know.

f. Whenever possible, employ methods for controlling access (e.g., callback, token generations, etc.).

g. An IS that has remote access capability will have a “Time-Out” protection feature that automatically

disconnects the remote device after a predetermined period of inactivity has elapsed. Twenty minutes is an acceptable norm.

h. Access should be denied after three unsuccessful log-on attempts. Users should not be re-instated until the IASO or the designee has verified the reason for the failed log-on attempts.

2-39. Employee Owned Computers and Off-Site Processing

a. The use of personally-owned hardware and software for government work is strongly discouraged; however, it may be used for processing unclassified and SBU information with DAA approval. Approval is based on the following requirements.

(1) The written approval will specify the conditions under which the IS will operate and the duration of the approval. An operating instruction, policy letter, etc., may provide "blanket" approval for a group of users.

(2) When a personally-owned IS is operated outside the work environment, make sure government-owned SBU information remains on removable media, and is marked and protected according to the SBU category (e.g., Privacy Act, FOUO, etc.) program directives.

(3) Take action to eliminate the need for personally-owned hardware and software. This could include purchase of additional hardware and software, realignment of current resources, reassignment of duties, and so forth.

(4) Consider the mission impact on loss of the resource. If a significant effect is evident, develop a plan with procedures for continued support (without personally-owned resources).

(5) It is a user's responsibility to virus scan all magnetic media (including personally-owned media) on the personally-owned IS. Whenever possible (depending on availability and copyright stipulations) the user's organization should provide and maintain the user's virus protection software.

b. Contractor owned or operated hardware and software must meet all security requirements for government-owned hardware and software.

2-40. Government–owned notebook computers. For government –owned notebook computers accredited to process classified information, the user will carry a copy of an accreditation letter while TDY or at an off-site location.

CHAPTER 3

CERTIFICATION & ACCREDITATION

DEVELOPED BY COMMITTEE # 7

3-1 Introduction

a. Purpose. Provides the implementation guidance of the Certification and Accreditation (C&A) policy as prescribed by AR 25-IA and the application of Department of Defense Instruction (DODI) 5200.40 Department of Defense Security Certification and Accreditation Process (DITSCAP). This guidance applies to Generic and Operational accreditations. The DITSCAP includes a risk management process. Implementation of the DITSCAP and this pamphlet fulfills the AR 25-IA policy requirements for both Certification and Accreditation (C&A) and Risk Management.

b. Definitions:

(1) Certification. Certification is the comprehensive evaluation of the technical and non-technical security features of an Information System (IS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design implementation meets a set of specified security requirements.

(2) Accreditation. Accreditation is the formal declaration by the Designated Approval Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

(a) Generic. Under the generic approach, systems fielded to multiple users are accredited as a single entity prior to fielding. While generic accreditations will lessen the administrative burden for the field users, local Information Assurance (IA) officials must still ensure that IS under their purview are operating under the terms of the generic accreditation. The generic accreditation will be applied to IS fielded under the Program Executive Office/Program Manager (PEO/PM) structure. Additionally, generic accreditation are appropriate whenever a single office or agency is responsible for fielding an IS to multiple Army users. The Information Assurance Security Officer (IASO) integrates new IS into the established architecture and ensures that the new IS do not adversely affect previously certified and accredited IS.

(b) Operational. Operational accreditation is applicable to all IS that have not been accredited by a generic accreditation. Operational accreditation is also required for IS covered by a generic Accreditation if the IS operates beyond the security bounds of the generic accreditation. The site-based approach to accreditation may be used for operational accreditation in accordance with paragraph 3-10, AR 25-IA.

(c) Site-Based Approach. Under a site-based approach, the entire site as defined and documented may be certified and accredited as a unit if the individual IS and components have been appropriately certified or accredited by a DAA. All Department of Defense Intelligence Information System (DODIIS) IS and networks processing Sensitive Compartmented Information (SCI) for which Defense Intelligence Agency (DIA) is the DAA will be certified and accredited using the site-based accreditation methodology detailed in DIAM 50-4.

c. Key Personnel. The IASO in coordination with the Information Assurance Manager (IAM) identifies and documents in the System Security Authorization Agreement (SSAA) the appropriate key personnel listed below.

(1) Designated Approving Authority (DAA or Accreditor). Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

(a) The DAA is appointed for operational accreditation, as follows:

[NOTE: AR 25-IA, para 2.3b states that protection levels replace modes of operation. At present there is no mapping of protection levels to modes of operation. Therefore, the modes of operation have been retained here until a clear mapping can be established.]

(1) The following individuals are accreditation officials for SCI and Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) systems:

(a) Dedicated SCI with no network connections. The Major Command (MACOM) commanders are the accreditation authorities for systems that process SCI and operate in the dedicated mode, provided these systems do not include external connections. General officers or a senior intelligence officer (SIO) authorized to authenticate correspondence for a MACOM commander may sign accreditation statements. A copy of each accreditation statement is

furnished to Commander, INSCOM (IAFM-TA), 8825 Beulah Street, Fort Belvoir, VA 22060-5246. The DCSINT is the accreditation authority for SCI systems not under the purview of a MACOM commander.

(b) Systems high SCI with no network connections. Systems high SCI with no network connections can be accredited by the MACOM. The Deputy Chief of Staff for Intelligence (DCSINT) is the accreditation authority for systems that process SCI in the systems high security mode with connection to external networks.

(c) Compartmented/multilevel or network connection SCI. The Director, DIA, is the accreditation authority for all systems that process SCI not covered by (a) or (b) above. The Director, National Security Agency) NSA, is the DAA for cryptologic systems under this mode of operation.

(d) SIOP-ESI. The Director, Joint Staff, is the accreditation authority for systems processing SIOP-ESI data. Requests for accreditation are prepared per MJCS 75-87 and forwarded through the Deputy Chief of Staff for Intelligence (DAMI-IM), 1000 Army Pentagon, Washington, DC 20310-1000.

(2) MACOM commanders and the Administrative Assistant to the Secretary of the Army (acting as the Headquarters, Department of the Army (HQDA) MACOM) are the accreditation authorities for Top Secret collateral systems operating in the dedicated, systems high, or compartmented security mode. The MACOM commanders and the Administrative Assistant to the Secretary of the Army may further delegate, in writing, accreditation authority to general officers, a MACOM Senior Intelligence Officer (SIO), or to Senior Executive Service personnel within their commands or agencies. Such delegation may be by name or by established position titles.

(3) The MACOM commanders and the Administrative Assistant to the Secretary of the Army are the accreditation authorities for Secret/Confidential systems operating in the dedicated, systems high, or compartmented security mode. The MACOM commanders (and the Secretary of the Army's Administrative Assistant) may further delegate, in writing, the accreditation authority to personnel at the minimum rank of colonel, GM-15, or GS-15 and who are occupying a position of command or of principal staff officer at an installation or general officer command. Such delegation may be by name or by established position titles.

(4) The MACOM commanders and the Administrative Assistant to the Secretary of the Army are the accreditation authorities for sensitive but unclassified (SBU) systems operating in the dedicated or system high mode of operation. Additionally, MACOM commanders and the Administrative Assistant (AA) to the Secretary of the Army may delegate, in writing, accreditation authority to other personnel who are in the minimum rank of lieutenant colonel, GM-14, or GS-14.

(b) DAAs are appointed for generic accreditation as follows:

(1) The Director, DIA, is the DAA for systems processing SCI that meet the following criteria:

(2) Operate or are planned to operate in the compartmented or multilevel security mode or that require connection to an external network, regardless of security mode.

(3) Have received special approval from DIA for a generic accreditation. This approval applies only to systems being fielded in identical configurations at a large number of sites. The DIA may

require additional measures such as configuration control.

(4) The DCSINT is the DAA for SCI systems not covered by (a) and (b) above.

(5) The Director of Information Systems for Command, Control, Communications, and Computer (DISC4) is the DAA for Top Secret and below IS in the multilevel security mode.

(6) The applicable PEO, with concurrence from DISC4, is the DAA for systems in the dedicated, systems high, or compartmented security mode. When a generic accreditation is appropriate and the IS is not being fielded through the PEO structure, a general officer or a member of the Senior Executive Service who has responsibility for fielding the system may be appointed as the DAA with concurrence from DISC4.

(7) If a generic accreditation is appropriate and the DAA is not readily apparent from the above guidance, DISC4 should be contacted for assistance to determine the DAA.

(8) Accreditation of the Signal Intelligence (SIGINT) system is the responsibility of the Director, NSA.

(2) Certification Agent (CA). The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an Information Technology (IT) system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.

(a) The CA is appointed by the DAA and shall be independent from the organization responsible for the system.

(b) The roles and responsibilities of the CA are defined, at a minimum, in Enclosure 4, DODI 5200.40.

(3) Program Manager (PM). The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the IT system. The roles and responsibilities of the PM are defined, at a minimum, in Enclosure 4, DODI 5200.40.

4. (4) User Representative. The individual or organization that represents the user or user community in the definition of information system requirements. The roles and responsibilities of the User Representative are defined, at a minimum, in Enclosure 4, DODI 5200.40.

(5) Information Assurance Security Officer (IASO). The IASO is responsible for developing the SSAA. The person responsible to the DAA for ensuring the security of an IT system is approved, operated, and maintained throughout its life-cycle in accordance with the SSAA.

3-2 Certification & Accreditation (C&A)

a. DITSCAP Overview

(1) This guidance implements the DITSCAP which establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit IT systems that will maintain the security posture of the Defense Information Infrastructure (DII). The DITSCAP focuses on protecting the DII by presenting an infrastructure-centric approach for C&A. The DITSCAP is designed to be adaptable to any type of IT and any computing environment and mission. The process should be adapted to include existing system certifications and evaluated products. This process is applicable to generic and operational accreditations.

(2) The process is designed to certify that the IT system meets the accreditation requirements and that the system will continue to maintain the

accredited security posture throughout the system life-cycle. The users of the process shall align the process with the program strategy and integrate the process activities into the system life-cycle. While DITSCAP maps to any system life-cycle process, its four phases are independent of the life-cycle strategy.

(3) The key to the DITSCAP is the agreement between the IT system program manager, the DAA, the CA, and the user representative. These managers resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the SSAA that is used to guide and document the results of the C&A. The objective is to use the SSAA to establish a binding agreement on the level of security required before the system development begins or changes to a system are made. In addition to the program manager, the DAA, the CA, and the user representative the process is supported by the Army IA personnel structure.

(4) The term program manager will be used throughout this document to refer to the acquisition organization's program manager during the system acquisition, the system manager during the operation of the system, or the maintenance organization's program manager when a system is undergoing a major change. The DAA is also referred to as the accreditor throughout this document.

b. Certification & Accreditation Process. The certification and accreditation process will be accomplished in accordance with Enclosure 3 and 4, DODI 5200.40.

c. Site Based Accreditation.

(1) Under the site based approach, the certification and accreditation focus may include a single system or network (as in the case of a complex, newly deployed system) or it may include smaller groupings of equipment as listed below:

(a) A local area network (LAN) can be accredited as a single unit. Individual personal computers and work stations on a LAN need not be accredited individually.

(b) Groups of stand-alone personal computer systems, work stations, and office automation systems located in the same general area and performing the same general functions may be accredited as a single unit.

(2) Under a site based approach, the entire site as defined and documented may be certified and accredited as a unit if the individual IS and components have been appropriately certified or accredited by a DAA. A site boundary is not limited to a specific geographic location and more than one site may be established at a single location (for example, Fort Bragg, North Carolina (NC), has five sites). A site may contain one or more systems and may also contain systems previously accredited by another DAA (for example, Central Intelligence Agency (CIA), NSA, other MACOM commanders, or their representatives).

(3) All DODIIS IS and networks processing SCI for which DIA is the DAA are certified and accredited using the site-based accreditation methodology detailed in DIAM 50-4. Specific guidance for establishing DODIIS Computer Security (COMPUSEC) sites is provided in DIAM 50-4 and its three supplemental documents:

(a) Site Information Assurance Security Officers (SITE IASO) Handbook.

(b) Developers Guide for Building a Certifiable and Accreditable System.

(c) A Certifier's Guide.

(4) When practical, the Army may establish sites composed of nonsensitive, SBU, collateral, and SCI systems.

(5) The ODCSINT Intelligence Information Management Directorate (DAMI-IM), in conjunction with the accrediting authority, cognizant Information Assurance Program Manager (IAPM), and site security personnel, determines whether a system or site-based approach applies to any given location. This determination is based on several factors, including but not limited to the following site criteria:

(a) Organizational structure and relative size.

(b) IS/network architecture density and complexity.

(c) Information Assurance Manager (IAM) staff capabilities.

(d) Commonality or uniqueness of IS/network components.

(e) Anticipated near-term and future IS/network modifications.

(6) The following actions are required to establish a site:

(a) The IAM and IASO, in conjunction with the appropriate commander, establishes a Configuration Management/Control Board to ensure that IS and networks included in the Site baseline can be securely maintained. The Configuration Management/Control Board consists of information management, acquisition, operations, security, and user management personnel and IA personnel.

(b) New SCI systems integrated into the site baseline meets the certification requirements of the DIAM 50-4.

(c) The site may include stand-alone systems and networked systems that directly and indirectly support an organization's mission.

(d) Site boundaries may include IS and networks not geographically located at the site if those systems are accessible via accredited network.

(7) The IS, guard devices, or networks intended to operate in the compartmented or multilevel security mode is given the highest priority for certification and accreditation due to the increased risk associated with their operation.

(8) The ISs and networks are certified and/or accredited on an individual basis to determine whether they operate at an acceptable level of risk under both the system and site based approach.

3-3. Reaccreditation

a. All accredited IS are reaccredited within 3 months following any of the events listed below:

(1) Addition or replacement of a major component or a significant part of a major system.

(2) A change in classification level of information processed.

(3) A change in security mode of operation.

(4) A significant change to the operating system or executive software.

(5) A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation.

(6) A significant change to the physical structure housing the IS that could affect the physical security described in the accreditation.

(7) The passage of 3 years since the effective date of the existing accreditation.

(8) A significant change to the threat that could impact Army systems.

(9) A significant change to the availability of safeguards.

(10) A significant change to the user population. E.g. all United States (U.S.) to U.S. and foreign nationals, etc.

(b) Reaccreditation includes the same steps accomplished for the original accreditation; however, those portions of the documentation that are still valid need not be updated.

(c) Reaccreditation of IS and networks that have been included in an infrastructure under the site based accreditation (SBA) concept (paragraph 3-10, AR 25-IA) is not required. The IS and networks are maintained under the configuration management requirements and compliance validation techniques provided in the SBA concept.

3-4. Interim Approval to Operate (IATO) before Accreditation. A DAA may grant an interim approval to operate for up to one year period before a generic or an operational accreditation is issued, provided the following conditions are satisfied:

a. A security survey has been performed and measures to prevent compromise, loss, misuse, or unauthorized alteration of data are deemed adequate. Some limitations on operations may be necessary during the period of interim approval.

b. An SSAA has been developed and procedures, manuals, or Standing Operating Procedures (SOPs) are provided to instruct the users on secure IS operations.

c. Applicable Communication Security (COMSEC) (Chapter 4, AR 25-IA) and TEMPEST (AR 381-14) requirements have been met.

d. A schedule for completion of requirements is established and agreed to by the DAA.

e. An interim approval to operate (IATO) may be granted to support a specific date or event (e.g., an exercise or awaiting Site Based Accreditation).

3-5. Certification and Accreditation Documentation

a. Documentation for the SSAA will follow the format (Appendix E (Outline) and Appendix F (template)) and include applicable appendices as referenced in Enclosure 6, DODI 5200.40. Instructions for completing the SSAA is contained in DOD 5200.40-M, DITSCAP Application Document, 20 Dec 98.

b. The following information is required in support of any Army accreditation. It will be included within the SSAA or as separate appendices or enclosures as follows:

(1) Concept of Operations Diagram (Required and described in the DITSCAP)

(2) Threat Statement (Required and described in the DITSCAP)

(3) Hardware/Software List (Required and described in the DITSCAP)

(4) ITSEC System Class (Required and described in the DITSCAP)

(5) Certification Analysis Level (Required and described in the DITSCAP)

(6) Technical and Non-Technical Security Requirements List (Required and described in the DITSCAP)

(7) Certification Team Member Roles and Responsibilities (Required and described in the DITSCAP)

(8) Tasks and Milestones (Required and described in the DITSCAP)

(9) Schedule Summary (Required and described in the DITSCAP)

(10) SSAA Roles and Responsibilities (Required and described in the DITSCAP)

(11) IASO Appointment Orders (Required by AR 25-IA and DA Pam 25-IA. Self-Explanatory)

(12) Standing Operating Procedures (Required by AR 25-IA and DA Pam 25-IA. The Standing Operating Procedures provides personnel with the administrative and security policy and procedures to be followed locally. The SOP addresses items such as media marking, handling, and protection; password management and protection; anti-viral product settings and use; security incident reporting; physical security; security training and awareness program for end users; etc.)

(13) Technical Security Configurations of Devices Enforcing a Security Policy (Required by AR 25-IA and DA Pam 25-IA. This appendix captures the security configuration and documents the security policy that is being enforced by the automated system.)

(14) Configuration Management Plan (Required and described in the DITSCAP)

(15) Risk Management Review (Required by AR 25-IA and DA Pam 25-IA.)

(16) Certification Test Plan/Procedures (Required and described in the DITSCAP)

(17) Certification Results/Recommendation (Required and described in the DITSCAP)

(18) Waivers (Required by AR 25-IA and DA Pam 25-IA. Self-explanatory.)

(19) DAA Accreditation Statement (Required by and described in the DITSCAP and in AR 25-IA and DA Pam 25-IA.)

CHAPTER 4: COMMUNICATIONS SECURITY

(DEVELOPED BY COMMITTEE # 8)

HOLD PLACE FOR CHAPTER 4 INPUT.

CHAPTER 5: RISK MANAGEMENT

(DEVELOPED BY COMMITTEE # 7)

5-1. Risk Management. The four phases of risk management as defined in AR 25-IA are implemented through the following activities. The activities are repeated as applicable throughout the system life-cycle and the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) (Department of Defense Instruction (DODI) 5200.40). During DITSCAP phase one the Designated Approval Authority (DAA), Program Manager (PM), Certification Authority (CA) and user representative determine the level of effort and plan for conducting risk management and document their results as an Appendix of the System Security Authorization Agreement (SSAA).

a. Overview.

(1) The most effective protection for Information System (IS) handling classified or sensitive but unclassified (SBU) information is through a risk management program. The objective of risk management is to achieve the most effective safeguards against deliberate or inadvertent activities as listed below:

(a) Unauthorized disclosure of information.

(b) Denial of service or use and running in a degraded mode.

(c) Unauthorized manipulation of information.

(d) Unauthorized use.

(2) Risk management of information systems is the process of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. The potential cost for broadly applied, marginally effective security features is enormous and underlines the need for effective risk management. Its application assists in optimizing the security return for each dollar invested.

(3) There are three basic choices in risk management:

(a) Risk avoidance. This choice is the most costly and should not be considered, since it requires the implementation of exorbitant countermeasures to nullify the risk and to protect information.

(b) Risk reduction and residual risk acceptance. This choice supports applying cost effective security measures to IS operations. The amount of risk that remains after the selection of a safeguard or countermeasure is known as residual risk.

(c) Total risk acceptance. While providing the least costly alternative at the onset, this choice may cost significantly more in the long run. Failure to implement security safeguards on an IS leaves its vulnerabilities open to exploitation by the local threats. In an operational combat environment, however, this level of risk may be acceptable to the combat commander in the short-term.

b. Definition.

(1) Risk Management. The process of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. The potential cost for broadly applied, marginally effective security features is enormous and underlines the need for effective risk management. Its application assists in optimizing the security return for each dollar invested.

(2) Threat. Any circumstance or event with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

(3) Vulnerability. Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.

(4) Assets. The totality of the components that make up the system or network. E.g. hardware, software, firmware, facilities, personnel, procedures, etc.

(5) Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

(6) Countermeasure. Action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

(7) Risk Assessment. Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting assessment is used as a basis for identifying appropriate and cost effective measures.

(8) Vulnerability Assessment. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security

measures, and confirm the adequacy of such measures after implementation.

(9) Residual Risk. Portion of risk remaining after security measures have been applied.

c. Risk Management Process.

(1) An effective risk management program entails a four-phased evaluation effort:

(a) Phase 1. Risk assessment of resources, controls, vulnerabilities, and threats.

(b) Phase 2. Management decision to implement security countermeasures and to accept residual risk.

(c) Phase 3. Implementation of countermeasures.

(d) Phase 4. Periodic review of the risk management program.

(2) The areas of software, hardware, procedures, communications, emanations, personnel (the highest risk), and physical security should be included in the risk assessment. Whenever possible, subject matter expert (SME) for the above areas or risk management software is used to enhance the process.

(3) Risk assessment involves estimating or determining loss potential that exists as the results of threats and vulnerabilities matching one another and causing some form of impact on the system. Using mathematical tools and statistical analysis techniques to determine the overall risk of operating a particular IS or network would seem to be a logical methodology to employ. However, experience shows that attempts to develop absolute models, performance simulators, or descriptive algorithms have been, at best, only marginally successful. These techniques should not be employed except when their value has been established. In many cases, qualitative or subjective techniques are more applicable to risk assessments performed for IS.

d. Risk Assessment

(1) Areas of assessment. Risk is determined from the analysis of vulnerabilities, threats, security requirements, and available safeguards for IS assets. After the analysis is complete and the chosen safeguards are in place, a security posture statement and recommendations to the DAA are written. Many automated tools are available to perform the risk assessment. These tools can reduce the manpower required to perform a risk assessment. The paragraphs below provide a brief summary of the entire risk assessment process.

(2) Assets identification. The cornerstone of any risk assessment depends on accurate identification of assets requiring protection.

(3) Vulnerabilities identification. System vulnerabilities are weaknesses in design, system security procedures, implementation, and internal controls that could be exploited by authorized or unauthorized users. Vulnerabilities identified either by inspection or notification and which are not corrected must be identified in all future risk assessments (for example, reports of The Inspector General, provost marshal, management review teams, evaluation teams, or Operations Security (OPSEC) evaluations). . See Appendix C for examples of vulnerabilities.

(4) Threat identification. Threat identification accounts for both known and reliably projected threats. A threat may be defined as an event or method that can potentially compromise the integrity, availability, or confidentiality of automated information systems. Threats include but are not limited to the following items:

(a) Foreign intelligence services, which may recruit authorized users or

employ unauthorized users to penetrate the system's safeguards. The Defense information infrastructure and Army systems that contain research and development, new technology, economic, and military operations data are of great interest to Foreign Intelligence Service (FIS) organizations. The local counterintelligence field office and local office of the Federal Bureau of Investigation must be contacted during the risk assessment process to assist in properly identifying all threats posed by foreign intelligence services.

(b) Deliberate or inadvertent error by authorized or unauthorized users. Computer viruses, malicious software, and programs designed to bypass security programs are examples of deliberate error. Accidental erasure of data by an authorized user is an example of an inadvertent error.

(c) Curious unauthorized intruders who have no FIS connections.

(d) See Appendix D for additional examples of threats.

(5) Threat and vulnerability matching. Threats are always present but can only affect an IS when a vulnerability or security weakness is present. The matching or pairing of a vulnerability with a threat is evaluated to determine the level of impact of risk. The level of risk may be measured by determining the possible rate of occurrence.

(6) Security requirements identification. Each security requirement drives the implementation of a countermeasure to reduce the occurrence of a vulnerability. The security requirement is the justification for the implementation of a safeguard.

(7) Countermeasure selection. At least one countermeasure should be developed for each threat and vulnerability match. A cost for each safeguard is estimated. Such countermeasures should not be limited to hardware and software fixes. Personnel, physical, and other possible procedural solutions should also be explored.

(8) Security posture comments and recommendations. A security posture statement is developed by summarizing the countermeasure selected to meet the security requirements. This statement is provided to the DAA with comments and recommendations such as those listed below:

(a) Accredit the IS or local area network (LAN) for processing in a particular mode of operation for a certain classification level. (This should be recommended when the security posture of the IS or LAN is very high and when the residual risk is at an acceptable level.)

(b) Grant an interim approval to operate (IATO) for a period of up to one (1) year while additional security safeguards are installed. (This recommendation should be made when the security posture of the IS or LAN requires enhancement due to a high level of residual risk.)

(c) Deny approval to operate. (This recommendation should be made when the IS or LAN has a very low security posture and the residual risk is unacceptable.)

e. Management decision to implement countermeasures

(1) The review of the security posture statement and recommendations are a responsibility of commanders or managers who rely on advice from ISS, counterintelligence, physical security, and other functional area experts. Identifying areas of exceptional or unacceptable risk is directly related to the organizational mission, goals, and objectives as stated by the commander or manager. At this point in the risk management process,

commanders can influence the commitment of resources to obtain the most effective security countermeasure and financial return on the investment. This assessment may reveal areas where reduced security is appropriate, based upon a low level of risk to mission objectives. These savings may then be applied to other security requirements.

(2) The selection of security controls includes a consideration of functional, technical, and economic feasibility and operational efficiency. Security requirements generally broaden managerial, operational, and administrative procedures, and in some cases, separate expenses occur that are directly attributable to these requirements. Only the commander or DAA can properly judge and balance the additional expense of security against operational efficiency. Commanders and organizational leadership must completely understand the impact of IS on mission accomplishment and the risks involved in operating the IS. The commander or DAA must, therefore, resolve any perceived conflict between operational and security considerations.

(3) If existing risks are determined to be unacceptable and require countermeasures impractical or impossible to implement, the commander or DAA should terminate the operation of the system.

(4) If penetration testing is a countermeasure to be employed, see Army Regulation (AR) 380-53 for policy requirements.

f. Implementation of countermeasures. An effectively applied risk assessment should lead to a series of interrelated countermeasures to be implemented according to a plan approved by the commander or DAA. The commander or DAA must always participate in this process because of the risk resulting from growing dependence upon IS.

g. Periodic review of the Risk Management Process. Organizational and operational dynamics demand a continuous review of the risk management program for effectiveness. Commanders must be assured that controls are providing the desired results. This process is an important step in ensuring the documented security techniques have not created a more serious vulnerability or risk. The collective effectiveness of applied countermeasures is the basis for future security actions that assist in identifying problem areas and additional security requirements.

APPENDIX A
References

Section I
Required Publications

AR 380-5
Department of Army Information Security Program.

AR 380-67
Department of the Army Personnel Security Program.

(S) DCID 6/3
Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U). This publication may be obtained from DIA (SY-ID), Bolling Air Force Base (Building 6000), Washington, DC 20340-0001.

(C) DIAM 50-4
Security of Compartmented Computer Operations (U). This publication may be obtained from the DIA address above.

(C) DIAM 50-5

Sensitive Compartmented Information (SCI) Contractor Administrative Security VOL I and VOL II (U). This publication may be obtained from the DIA address above.

(C) DOD Pub C-5030.58-M
Security Criteria and Telecommunications Guidance.

DODI 5200.40
Department of Defense Security Certification and Accreditation Process (DITSCAP). Cited in Chapter 3.

Executive Order 12958
Classified National Security Information, April 17, 1995.

Information Systems Security Products and Services Catalogue. This publication may be obtained from the Superintendent of Documents, U. S. Government Printing Office, WASH, DC 20402.

JCS 6-03.7
Security Policy for the GCCS Intercomputer Network.

NCSC-TG-005
Trusted Network Interpretation. This publication may be obtained from the Superintendent of Documents, U. S. Government Printing Office, WASH, DC 20402.

17 USC 506
Copyright Infringement

Section II
Related Publications
A related publication is merely a source of additional information the user does not have to read to understand this regulation.

AR 15-6
Procedures for Investigating Officers and Boards of Officers.

AR 25-1
The Army Information Resources Management Program.

AR 25-400-2
The Modern Record Keeping Systems (MARKS)

AR 36-5

AR 70-1
Systems Acquisition Policy and Procedures.

AR 105-64
U.S. Army Communications Electronics Operation Instructions Program (CEOI).

AR 190-13
The Army Physical Security Program.

AR 190-51
Security of Unclassified Army Property (Sensitive and Nonsensitive), 30 Sep 93.

AR 310-25
Dictionary of United States Army Terms.

AR 25-30
U S Army Contingency Planning Program

AR 25-55
The Department of the Army Freedom of Information Act

AR 340-21
The Army Privacy Program.

(C) AR 380-28
Department of Army Special Security System

AR 380-40
Policy for Safeguarding and Controlling Communication Security (COMSEC) Material

AR 380-53
Communications Security Monitoring.

(C) AR 380-381
Special Access Programs (SAPs).

AR 381-10
U.S. Army Intelligence Activities.

AR 381-12
Subversion and Espionage Directed Against U.S. Army (SAEDA)

AR 381-14 (S)
Technical Surveillance Countermeasures (TSCM and TEMPEST) (U).

AR 381-20
U.S. Army Counterintelligence Activities.

AR 525-13

AR 525-20
Information Warfare/ Command and Control Warfare (IW/C2W) Policy

AR 530-1
Operations Security (OPSEC).

AR 25-12
Criteria for Insuring the Competency of Personnel to Install, Repair, and Maintain Communications Security Equipment.

CSC-STD-003-85
Computer Security Requirements.

CSC-STD-004-85
Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements.

DA PAM 25-380-2
Security Procedures for Controlled Cryptographic Items (CII)

DCID 1/21
Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), July 29, 1994.

DIAM 50-24, Secure Communications for the Operations of Secure Telephone Units (STU-III) and Modems with a Sensitive Compartmented Information Facility (SCIF)

DoD 5200.1
DoD Information Security Program Regulation

DOD Instruction 5215.2
Physical Security Technical Vulnerability Reporting Program
(CSTVRP).

DOD 5200.22-M
Industrial Security Manual for Safeguarding Classified Information.

DOD 5220.22-R
Industrial Security Regulation.

(S/NF/WN) DST-1750S-208-93, Threats to U.S. Army Tactical, Strategic, and Sustaining Base Information

Federal Standard 1027
General Security Requirements for Equipment Using the Data Encryption Standard.

FIPS Pub 31
Guidelines for Automatic Data Processing Physical Security and Risk Management.
FIPS Pub 65
Guidelines for Automatic Data Processing Risk Analysis.

(S) MJCS 75-87
Safeguarding the Single Integrated Operational Plan (U).

NCSC-TG-001
A Guide to Understanding Audit in Trusted Systems.

NCSC-TG-003
A Guide to Understanding Discretionary Access Control in Trusted Systems.

NCSC-TG-006
A Guide to Understanding Configuration Management in Trusted Systems.

NCSC-TG-007
A Guide to Understanding Design Documentation in Trusted Systems.

NCSC-TG-025, Version 2
A Guide to Understanding Data Remanence in Automated Information Systems.

NSTISSI No. 4009
National Security Telecommunications and Information Systems Security Council (NSTISSI), "National Information Systems Security (INFOSEC) Glossary

NTISSM 2-90
COMPUSEC

ODCSINT Pamphlet 380-25-1
Accreditation Handbook for U.S. Army DoD Intelligence Information Systems (DODISS) Intelligence Automated Information Systems (AIS) and Networks Processing Sensitive Compartmented Information (SCI)

(S/NF/WN) SPB 145-95, Intelligence Community and Related Automated Information Systems and Networks: Vulnerabilities and Threats (U)

Director of Information Systems for Command, Control, Communications, and Computers

Keeping the Highway Open and Secure for Force XXI
Volume I: The Army C2 Protect Program Management Plan (PMP), Volume II: The Army C2 Protect Master Training Plan (MTMP), Volume III: The Army C2 Protect Implementation Plan

APPENDIX B

Management Control Evaluation Checklist

B-1. Function

The function covered by this checklist is the administration of the Army Information System Security Program.

B-2. Purpose

The purpose of this checklist is to assist Assessable Unit Manager and Management Control Administrators in evaluating the key management controls outlined below. It is not intended to cover all controls.

B-3. Instruction

Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, sampling, simulation, or others). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2-R (Management Control Evaluation Certification Statement). A locally reproducible copy of this form is located at the back of this publication.

B-4. Test questions

a. Are appropriate security personnel (for example, ISSPM, ISSM or ISSO) appointed?

b. Are risk analysis/vulnerability assessments performed at the appropriate levels for systems that process Army information?

c. Are the appropriate leadership/management personnel aware of the results of risk analysis/vulnerability assessments?

d. Are countermeasures identified based on the results of risk analysis/vulnerability assessments?

e. Are countermeasures in place commensurate with risk/vulnerability?

f. Is there a written security plan to document implementation of countermeasures?

g. Has leadership/management formally accepted the risk to process the information involved? (Are the systems accredited?)

h. Are countermeasures routinely tested (for example, user IDs, passwords, audit trails)?

i. Is Information System Security training performed at appropriate levels?

j. Are MACOMs, installations, or activities funding their INFOSEC requirements under the appropriate MDEP?

k. Are security incidents/violations (for example, viruses, unauthorized entries or attempts) reported and investigated?

l. Have plans been developed to ensure continued operation in the event of major disruption (for example, fire, natural disaster, bomb threat, civil disorder)?

m. Has a configuration control board approved each network? Is there an appropriate security official as a member of each board?

B-5. Supersession

This checklist replaces the checklist for Intelligence Activities/Army Information System Security Program (AISSP) previously published in DA Circular 11-92-1.

B-6. Comments

Help to make this a better tool for evaluating management controls. Submit comments to: Director of Information Systems for Command, Control, Communications, and Computers (SAIS-PAC), 107 Army Pentagon, Washington, DC 20310-0107.

APPENDIX C

CONTINUITY OF OPERATIONS PLAN
EMERGENCY READINESS
EVALUATION QUESTIONNAIRE
FOR
COMPUTERS, LOCAL AREA NETWORKS
AND OPERATIONAL SERVICES

EVALUATION

This is a sample emergency readiness evaluation, which can be conducted on all Continuity of Operations Plans to document their status. This evaluation is designed to help determine plans in place and identify planning that remains to be done. The evaluation will be conducted through the series of attached questionnaires. The following instructions are provided to assist the responsible operational service or LAN disaster planning manager in answering the evaluation questions, and aid in the interview process. The questions should be answered "Yes," "In Process," or "No," .

1. A YES (Y) answer indicates that the item in question exists, is adequate and is current, etc.

2. An IN PROCESS (IP) answer indicates that the item exists but is incomplete, out-of-date etc. "IP, but . . . . . ."

3. A NO (N) answer indicates that the item does not exist at all!

If a question does not apply because of "NO" answer to a previous question, answer "NO." For example:

a. Is there *a formal* written disaster recovery plan? NO
b. Is there a *formal distribution list* for the plan? NO

Answers to the questions will be analyzed and the progress of planning will be determined. The evaluation questions may be used to develop an action item list for the continuity of operations action plan.

EMERGENCY READINESS EVALUATION CHECKLIST

BACKUP FACILITIES & PROCEDURES **Y IP N**

Are backup files maintained at a secondary site? .....
Are duplicate program files stored off-site? .....
Are duplicate copies of documentation maintained? .....
Are copies of documentation stored off-site? .....
Are backup copies of documentation reviewed periodically
to assure applicability? .....
Is a backup service facility, contingent operations mode or
backup LAN available .....
Is the backup service facility or LAN in a different room or
building than the primary facility or LAN? .....
Can the backup facility handle the current workload? .....
If no designated backup exists, is there access to another
service facility, carrier, or LAN? .....
Is an implementation plan available for use of backup facility,
carrier, or LAN? .....
Have formal contingency plans been developed for service
facility or backup capability? .....

CONTINGENCY PROCEDURES **Y IP N**

Has it been determined if manual processing of each critical
service function or LAN application is feasible and necessary? .....
Are there formal, written manual operating procedures for
each such critical service or LAN application? .....
Are there formal, written procedures for resuming operating
services and LAN-based applications after manual processing? .....
Have all manual processing procedures been tested? .....
Have all procedures for resumption of operational services
and LAN processing been tested? .....

RECOVERY PROCEDURES **Y IP N**

Have disaster recovery teams been defined? .....
Does each recovery team have written responsibilities and
procedures to follow? .....
Do recovery procedures cover each of the following:
Retrieval of all necessary files documentation etc. from
the off-site vault? .....
Activation of a backup facility, carrier or LAN if necessary? .....
Transportation of personnel supplies etc., to offsite
alternatives, if necessary? .....
Establishment of necessary communications and
telecommunications links? .....
Copying backup files and programs to the backup alternative? .....
Specific instructions for recovery of each service function
and critical LAN application? .....
Running a test to verify proper performance of hardware,
software and communication/telecommunications links? .....
Determining a schedule for interim restoration of service

functions and processing of critical LAN applications? .....
Liaison with users? .....

Return to normal operations and processing when the primary service facility or LAN is fully restored? .....

EVENT DETECTION **Y IP N**

Are there specific procedures for responding to emergencies (fires. bomb threats etc.)? .....
Are emergency procedures readily available in the service facility? .....
Do emergency procedures include actions that pertain specifically to the operational service or LAN data? .....
Do emergency procedures specify persons to be contacted and their alternates? .....
Are there procedures or guidelines for escalating problems or interruptions to disaster status? .....

MANAGEMENT PROCEDURES **Y IP N**

Is there one person with management responsibility for disaster recovery? .....
Is there one person responsible for coordinating recovery operations? .....
Have recovery operation teams been defined, staffed and trained? .....
Is there a procedure for notifying the disaster management team? .....
Have specific locations been identified, either on-site and off-site (or both) to use as control centers for directing recovery operations? .....
Is there a procedure for conducting damage assessment? .....
Have the persons responsible for damage assessment been identified? .....
Is there a procedure for notifying the recovery LAN organization and mission-essential service users of steps to be taken? .....
Is there a current list of service facility and LAN personnel phone numbers? .....

INVENTORY **Y IP N**

Is there a current inventory of each of the following resources:

Hardware .....
Communications and telecommunications components .....
Data entry devices, if required .....
Firmware .....
Software .....
Data .....
Supplies .....
Does the inventory show which items are needed for critical service functions and LAN applications? .....
Is there a list of dependent carriers, hardware, software and other service vendors? .....

TRAINING **Y IP N**

Is there a systematic program for training on the continuity of operations plan? .....

Are records kept of which employees have received continuity of operations training? .....
Is the training program revised based on the results of recovery tests? .....
Are service facility and LAN staff given cross-training? .....
Is the continuity of operations plan used as the basis for training? .....

TESTING	**Y**	**IP**	**N**
Have the contents of the offsite vault been tested for adequacy within the past year?			
Are there procedures for testing restoration of services using inhouse service or LAN facilities and off-site files and documentation?			
Have recovery procedures been tested within the past year using inhouse facilities and off-site files and documentation?			
Have recovery procedures been tested within the past year using backup facilities and offsite files and documentation?			

MAINTENANCE	**Y**	**IP**	**N**
Is there a schedule for review and revision of the continuity of operations plan?			
Is there a procedure for initiating revisions to the continuity of operations plan?			
Are the results of testing reviewed for training implications?			
Are the results of training reviewed for planning implications?			

AR 25-IA

Policy Augmentation

Development of a Continuity of Operations Plan (COOP)
In the event of
Physical or Cyber Attack
on US Army Information System(s)

DRAFT Version 1.0
Dated 30 July 1999

General

1. Purpose

This document augments US Army Regulation 25-IA and establishes guidance for contingency operations of information systems. It is the intent to cover emergencies due to:

- ?? An information warfare or cyber attack;
- ?? Natural disasters;
- ?? Physical disruption of the processing portions of the information system; and
- ?? Inadvertent human error.

Implementation of this regulation ensures the continual readiness evaluation and for the intentional incorporation of new technologies to meet the changing cyber-threats and other emergency situations.

2. Explanation of Abbreviations and Terms

The following abbreviations and terms are used throughout this document.

a. CERT – Computer Emergency Response Team
b. Cold Start – A complete system reboot that assumes little or no information/data replenishment/recovery is possible. The system is either taken off-line and then restarted, or control and system functionality are picked up at the contingency site. This type of restart completely interrupts the real time flow of the system.
c. Data at Rest – Data contained within a database or resident within a given information system.
d. Data on the Move – Data that is in the process of being transmitted from one portion of a network to another portion.
e. DOIM – Directors of Information Management
f. Hot Start – A non-intrusive system restart that occurs without any intervention by the operator and usually without any knowledge of the user. This type of restart preserves all data and information in the system (both data at rest and data on the move) and maintains real time systems operation.
g. INFOCON – Information Operations Condition, which provides a measure of the focus on computer network-based protective measures, due to the nature of a computer network attack.
h. ISSM – Information System Security Manager
i. ISSPM – Information System Security Program Manager
j. ISSO – Information System Security Office
k. IP – Internet Protocol
l. I3A – Installation Information Infrastructure Architecture
m. LIWA – Land Information Warfare Activity
n. Op Cmmd – Operations Command
o. Priorities –The level of importance given to a particular item in order to facilitate the re-establishment of system capabilities for users

p. Service provider – Outside commercial Internet carrier
q. System DAA – Designated Accrediting Authority
r. TNOC – Theater Network Operations Centers
s. Warm Start – A system restart that requires some operator/administrator intervention and/or assistance. This type of restart preserves most of the information in the system and requires minimal down time to return to real time operations.

3. Responsibilities

This section of the regulation will show, for both sustaining base and tactical environment systems, the responsibilities of each major information systems owner/provider/manager against specific sub-products of the actual COOP. The table below defines the responsibilities of the cognizant systems owner/provider/manager.

Specific responsibilities	S	PEO	PM	ISSPM	ISSM	ISSO	TNOC	DOIM	System DAA	Op Cmmd
Develop a COOP for systems under direct control or ownership	X			X	X	X	X	X	X	X
Develop a COOP for systems and programs under development		X	X							
Program and fund COOP readiness		X	X	X	X	X		X		X
Review and provide approval/disapproval for non-government service providers to ensure there is a COOP in place with that provider.		X	X	X	X	X	X	X	X	X
Approve the development and maintenance of COOPs for all supported elements.		X	X	X	X	X	X	X	X	X
Maintain a list of approved COOPS.		X	X	X	X	X	X	X	X	X
Restrict root and system level access to only those individuals with a need to know.				X	X	X			X	X
Implement procedures and install and maintain software that ensures only authorized users with valid user IDs and passwords are granted access.	X			X	X	X	X		X	
Implement procedures and install and maintain software that monitors all users and maintains records of unauthorized attempts.	X			X	X	X	X		X	X
Designate a Systems Administrator/Systems Operator as the approval authority for all data files and applications residing on the system.		X	X	X	X	X			X	
Ensure all COOPS are accredited in accordance with requirements of AR xxx		X	X	X	X	X	X	X	X	X

and comply with requirements of AR xx.										
Contact the cognizant Security Program Manager or Installation Security Manager for specific automation and communications security guidance/ requirements.	X			X	X	X	X	X	X	X
Maintain licensing or approval documentation for all COTS software residing in the system				X	X	X	X	X	X	X
Not make available any commercial software for download.									X	
Stop an attack through the use of firewalls, gateways, and other techniques	X			X	X	X	X	X	X	X
Protect a system by predicting and detecting intrusions	X			X	X	X	X	X	X	X
Provide secure environments where access (both physical and electronic) is controlled	X			X	X	X	X	X	X	X
Collect and maintain electronic evidence of any unauthorized or unexplained system intrusions	X			X	X	X	X	X	X	X
Provide security measures anticipating that a system intrusion will occur			X				X			
Provide the means to analyze in real time the intent and focus of an attack									X	X
Provide for the recovery of data/information and restoration of the operating state of a system.	X	X	X	X	X	X	X	X	X	X

4. Mission

This section of the document describes the mission of the COOP policy. The primary mission is to describe the need for developing tactical and sustaining base COOPs in accordance with the method approved by the Headquarters, Department of the Army. The secondary mission is to provide an overview of the essential elements of the COOP to enable and facilitate COOP development.

Due to the changing threat scenario and the growing number of attacks on information systems, a COOP is a necessary element of all command operations. The presence of a COOP will help to ensure that systems remain in or regain operational status in the event of:

- ?? An information warfare or cyber attack;
- ?? Natural disasters;
- ?? Physical disruption of the processing portions of the information system; and
- ?? Inadvertent human error.

The essential elements of the COOP are those that define what steps need to be taken in the event that an emergency situation such as those listed above should occur. These essential elements are described below.

1. Responsibilities -- Detail the roles and responsibilities for various COOP activities. Cite the specific responsibilities and include the

organizational entity responsible for each activity. Ensure that each entity listed in the COOP understands their roles and responsibilities. Ensure that all the key players (e.g., system owner, data provider, manager, etc.) understand their roles and their interfaces with each other.

2. Contingencies or Risk Analysis -- Reference the vulnerability assessment and testing results procedure required for the system. Describe what actions need to occur depending upon the evaluated conditions determined by INFOCON levels.

3. Priorities -- Need to establish the priorities for re-establishing system operations in the event of an emergency. The priorities will change depending upon the current INFOCON level, the current phase of the conflict, and the type of emergency that has occurred. Because this problem has multiple dimensions making a top-to-bottom prioritization difficult, recommend including several scenarios that list priorities based on the situation.

4. Protection of Data and Information -- Delineate the requirements for access and control of the data, information, and software contained in the system. Describe the security devices used for protecting the system hardware including physical access levels, controls, and reporting mechanisms. Maintain a record of critical system information such as its physical and cyber configurations and its minimal essential data and information.

5. Detection -- Describe the implementation of devices that will detect unauthorized access to the system. This includes both physical and cyber devices. Provide a process for reporting both the suspicion and the confirmation of unauthorized access.

6. React -- Describe the methods for reacting to an emergency. The reactions will depend on the type of emergency and the severity of the INFOCON level.

7. Recover -- Provide methods for recovering a system following an emergency. Again, the method used will be event-driven: it will depend upon the type of emergency and severity of the INFOCON level. In the case of a cyber-attack, the recovery method will involve some sort of re-start of the system: co-operative, mixed, or non-cooperative.

8. Respond -- The response actions will take two forms. One will be a response in terms of alerts to the users of the system. Two will be a response to the reduced effectiveness of the system. Begin by quantifying the damage to the system. Then notify the responsible DOIM and collateral system DAA to initiate the response sequence.

9. Manage -- Prepare a back-up operations site in the event of an emergency. Include physical, data, information, and software redundancies. Determine and assign appropriate levels of maintenance activity for the back-up site.

5. Contingencies or risk analysis

This section describes the correlation between system vulnerabilities and actions to be taken as a result of those vulnerabilities being exploited. This section also describes the periodic required vulnerability testing and assessments that directly aid in the management and removal of information system vulnerabilities.

The local administrator, in conjunction with the systems owner, systems DAA, TNOC and DOIM, will ensure that a vulnerability assessment that contains the results of vulnerability testing (to include penetration testing) will be executed. The latest vulnerability assessment report will be maintained as a need-to-know report at both the local administrator level and the next level up.

All levels of systems responsibility will examine results of the vulnerability assessment and vulnerability testing. Each vulnerability will be addressed by an appropriate restart condition. These restart conditions are in the form of hot, warm and cold restarts, defined as follows. A hot restart is a non-intrusive systems restart that occurs without any intervention by the operator and usually without any knowledge of the user. This type of restart preserves all data and information in the system (both data at rest and data on the move) and maintains real time systems operation. A warm restart is a systems restart that requires some operator/administrator intervention and/or assistance. This type of restart preserves most of the information in the system and requires minimal down time to return to real time operations. A cold restart is a complete systems reboot that assumes little or no information/data replenishment/recovery is possible. The system is taken off-line and then restarted, thus interrupting the real time flow of the system and removing any knowledge from the system.

The local administrator, in conjunction with the systems owner, systems DAA, TNOC and DOIM, will ensure that the COOP addresses both the physical and cyber malfunction case. The following table describes the restart conditions expected as a result of general system failure conditions. The local administrator, in conjunction with the systems owner, systems DAA, TNOC and DOIM, will use this table as a guide in the preparation of the COOP.

Key to the preparation of the COOP is the cognizance of the potential for destruction, both physical destruction of system components and the cyber equivalent of destruction due to a cyber attack. For conventional warfare, these states are described as Defense Conditions (DEFCONs). There is a set of definitions for Information Operations (cyber destruction) that are the equivalent to DEFCONs (physical destruction). The levels for these Information Conditions are:

- ?? Normal – no significant cyber activity
- ?? Alpha – increased risk of an attack
- ?? Bravo – specific risk of an attack
- ?? Charlie – limited attack(s)
- ?? Delta – general attack(s)

All levels of systems responsibility will examine results of the vulnerability assessment and vulnerability testing and then include in the COOP the actions that would be taken to protect military information systems at the varying INFOCON levels. Those actions will include correlation of hot, warm, cold start options to the INFOCON levels.

6. Job or System priorities

This section delineates the importance of considering changes to the system priorities in the event of an emergency situation. Priorities – defined as the level of importance given to a particular item

in order to facilitate the re-establishment of system capabilities for users – can be determined by several means. These are:

?? The state of the emergency (i.e., INFOCON or DEFCON level)
?? The phase of military operation and deployment environment
?? The functional need for that application or business area (e.g., Logistics, Safety, etc.)

The Army Installation Information Infrastructure Architecture (I3A) lists 12 business areas whose capabilities must be prioritized as part of the COOP. These areas are:

1. Personnel/Human Resources
2. Safety
3. Medical
4. Acquisition Management
5. Information Technology Management
6. Logistics
7. Maintenance
8. Training
9. Finance
10. Engineering/Facilities Management
11. Installation Management (Base Operations)
12. Publication Distribution

Additional Command and Control (C2) functions will supplement this list.

The DOIM will ensure that system priorities will be considered and defined in the Continuity of Operations Plan (COOP).

7. Succession of Personnel

This section describes the chain of command to be followed in the event of information system loss due to either physical or cyber causes. This chain of command refers to the back-up designation of root level access to the system. The key issue is the id/password administration of portions of the system and networks that allow full system level controls and accesses. Particularly if there is to be a cold restart or a transfer of information systems processing to a backup site, the ability for local administrators to access all portions of the system is crucial. Protection of those accesses will be controlled on a need-to-know basis. Other specific succession of personnel requirements are as follows:

?? The DOIM will maintain a list of personnel who have been designated with access to systems routers, networks, and other areas of the information system.
?? All program managers and ISSMs will maintain a configuration list of areas of the system where password access is necessary.
?? Local administrators will ensure that the access list is current and accurate.
?? The system responsible owner and the local administrator will maintain a configuration versus access list that specifies all areas of the system where password access is necessary (this is not a list of passwords, rather a list of areas that require passwords).
?? All systems responsible owners and local administrators will ensure that no single file or physical location contains all passwords to the system.

II Protection of data and information

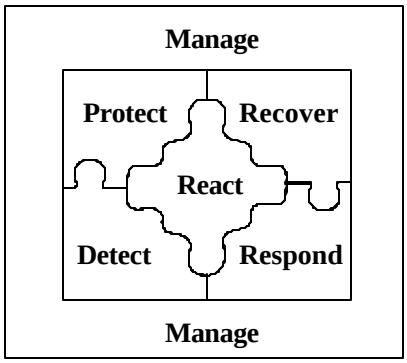
1. Pillars of Information Operations (Protect, Detect, React, Recover, Respond, Manage)

The focus of this augmentation of US Army Regulation 25-IA is to look at full spectrum protection in the event of a disruption of an information system due to either a cyber or physical event. To

provide that level of protection, defense-in-depth can be thought of as the combination and interaction of technologies that:

?? Stop an attack through the use of firewalls, gateways, and other techniques,
?? Protect a system by predicting and detecting intrusions,
?? Guarantee secure environments where access (both physical and electronic) is adequately controlled,
?? Collect electronic evidence, anticipating that a system intrusion will occur,
?? Analyze in real time the intent and focus of an attack, and
?? Provide for the recovery of data/information and restoration of the operating state of a system.

A complete defense-in-depth posture not only provides greater resiliency to a system, but also considers the integration of technologies that can enhance that resiliency. The figure below illustrates the cooperative nature of defense-in- depth as it relates to the recovery of: system operation, data and information compromised during either a physical or an IW event. The salient feature of this approach is that it provides measures beyond defensive IW into a more comprehensive information assurance posture.



The Interlocking Nature of Defense-in-Depth Technologies

What is most important is that a combination of cooperative strategies increases the resiliency of a system and facilitates the return to operation of that system after an IW attack. The overall point is to define the scope of a defense in depth posture that is required for each information system. There is the recognition that the technologies for both cyber defense and cyber offense will be constantly evolving. It is the intent of this document to require defensive functionality without specifying defensive applications by name.

2. Protection of Data and Information

This section describes the requirements for the protection and control of the data, information, and software contained in the information system. The intent is to specify required functionality and not specifically require an application by product name.

?? The systems administrator, the program manager, and the ISSM will ensure that access to program application code configuration is limited and controlled.
?? The systems administrator, the program manager, and the ISSM will establish procedures that provide constant monitoring for viruses and malicious code.
?? The ISSM and the systems administrator will ensure that access and monitoring records are maintained.
?? The systems administrator, the program manager, and the ISSM will ensure the implementation and integration of software access control.
?? The ISSM and the systems administrator will ensure that the system is protected from

unauthorized entry through an Internet Protocol (IP) service.

- The ISSM and the systems administrator will ensure that adequate cyber-safeguards exist at the commercial provider source (if required) to prevent unauthorized access to the system.
- The ISSM and the systems administrator will confirm that adequate cyber-safeguards exist to prevent unauthorized access to the non-IP portions of the system (e.g., sensors).

3. Protection of Physical Information System

This section describes the incorporation of physical access control and reporting. This contains the requirements for security devices that will be employed for all the hardware components (including processors, servers, client workstations, routers, networks, etc.) of an information system.

- The systems administrator, the program manager, and the ISSM will ensure that physical access to processing components of the information system is limited and controlled.
- The ISSM and the systems administrator will ensure that access and monitoring records are maintained.
- The systems administrator, the program manager, and the ISSM will ensure the implementation and integration of physical access control devices and software.
- The systems administrator, the program manager, and the ISSM will establish procedures that provide constant monitoring for viruses and malicious code.
- The ISSM, ISSO and Program Manager will evaluate anti-tampering as an additional method of protecting the physical assets of the system.

4. List of Records and Documentation

This section describes the requirements for maintaining critical information and data that will be used to restart the system after a physical or cyber attack. Critical to this is the identification and maintenance of two specific pieces of information. The first is the physical configuration of the information system. The second is known as the minimal essential data and information. This is defined as the smallest set of data and information that can be used to restart the system in real time.

- The COOP for all systems will identify the responsible person who establishes the procedure for maintaining correct and current configuration of the system (both hardware and software components).
- The systems administrator will determine the network and services requirements that support hot, warm, and cold restarts.
- The systems administrator will be responsible for determining the minimal essential data and information for the system and the ISSO will provide assistance.
- The ISSO and the ISSM will determine the manuals and documentation necessary for to support hot, warm, and cold restarts.

5. Safeguarding Essential Materials

This section will contain the requirements for ensuring that the minimal sets/data/information are protected against cyber attack. Typically this section contains a

reference requiring that this occur. It is most likely that the actual means of safeguarding the system and the techniques implemented will be controlled.

Detect

This section describes the requirements for implementing detection approaches looking for unauthorized accesses to the system. The detection approaches should take the form of both early warning (i.e., looking at information over a period of time) and more conventional approaches such as packet evaluation, etc. Examples of requirements are:

1. The ISSO/ISSM will ensure that the information system is protected from unauthorized entry through an IP service.
2. The PM and the system administrator will ensure that adequate cyber safeguards exist at the non-military service provider (is applicable) to prevent unauthorized access to the information system.
3. The ISSO will confirm that adequate cyber safeguards exist to prevent unauthorized access for the non-IP portions of the information system.
4. The information system defense will maintain records of anomalous behavior and catalog intrusion type and characteristics.
5. The records of anomalous behavior will be reported to collateral and higher level system.
6. The PM and the system administrator will ensure that a liaison with the US Army Land Information Warfare Activity (LIWA) Red Team, Computer Emergency Response Team (CERT), organic assistance personnel, and appropriate reporting channels is established.
7. The information system will monitor system activity, traffic, up/down-time, and other system characteristics to determine “normal” versus “anomalous” conditions.
8. Anomalous behavior will be reported to networked and higher level system administration and headquarters points of contacts.

React

This section describes the requirements for determining, implementing, and quantifying reactions in the event of an emergency. Reaction approaches are those activities that are done in reaction to an identified emergency, such as unauthorized access to the system or the physical loss of part or all of the system.

1. The system administrator, ISSO, and ISSM will ensure that access to the system has been closed in the event of a penetration that was reported by the detection portion of the system and that the attack is stopped.
2. Cyber deception approaches will be established by the appropriate level and coordinated with the DOIM. (Note: It is most likely that the actual means and the techniques implemented will be classified.)
3. The DOIM will coordinate and establish cyber-deception approaches (e.g., “honey-pots”) to help minimize damage to the system, identify system vulnerabilities, and facilitate identification of attackers.
4. If deception or forensics is necessary, the DOIM will be notified.
5. Provisions for the collection and retention of cyber forensic information will be established by the ISSM and program manager and coordinated with the DOIM.
6. The system will notify users in the event of the emergency situation and establish liaison with the US Army Land Information Warfare Activity (LIWA) Red Team, Computer Emergency Response Team (CERT), organic assistance personnel, and appropriate reporting channels.
7. The system administrator, ISSO, and ISSM will identify and address the vulnerabilities in the system that enabled the attack to occur (e.g., install software patch).

Recover

This section contains the requirements for determining, implementing, and quantifying recovery approaches in the event of an emergency. It is expected that the recovery re-starts will take one of three forms: co-operative (hot), neutral (warm), and non-cooperative (cold). It is further anticipated that the type of re-start that is executed will depend in part on the amount of damage done to the system during the emergency.

1. Cognizant system owners will ensure that:
   - ?? The system has a recovery plan (both automated and manual) that considers full and/or partial loss of system functionality.
   - ?? The recovery plan considers various scenarios.
   - ?? The recovery plan is structured to provide for cooperative (hot), neutral (warm), and non-cooperative (cold) restarts.
   - ?? In the event of a system crash, where it has been determined that contents in the data base have been overwritten, implement a cooperative re-start using data stored in the system.
   - ?? In the event that the system's communication capabilities are disabled, where it has been determined that the networks are overloaded, implement a neutral start. This would involve informing users of the emergency and then re-programming the system with the latest available information.
   - ?? In the event that the system's communication capabilities are disabled, where it has been determined that the router tables have been erased, implement a non-cooperative start using stored information in the system.
2. For new and modified systems development, the program manager will ensure that recovery approaches are designed into the system.
3. The assistance of US Army LIWA, the command security office, and other organic assistance personnel will be enlisted as required.

Respond

This section contains the requirements for determining, implementing, and quantifying responses in the event of an emergency. Respond is different from React (Section IV) in that React focuses on the activities that need to be accomplished in order to immediately address the emergency situation (e.g., shut-down an unauthorized access). Respond, on the other hand, focuses on the activities that are to be taken once the emergency is under control. Though not a comprehensive list, the following provides examples of requirements for incorporating response approaches.

- The DOIM and networked system administrators will be notified in the event of a system emergency.
- The DOIM and the systems administrator will decide based on the severity of the emergency, whether a move to back-up operations is required.
- The DOIM will notify the affected system administrator as to the go/no go or continuation of defensive deception technique operations.
- LIWA Red Team, CERT, vulnerability assessment team, organic assistance personnel, and others will be notified as appropriate.

Manage - Backup Operations

This section contains the requirements for the management of the backup operations of the information system. The purpose is to spell out the requirements for the type of restart (hot-warm-cold) versus the type of attack. Backup operations are expected to be necessary if the system under attack requires a complete reboot or is physically disabled. The alternate site needs to be maintained and planned for in the event of an unsuccessful restart.

Condition	Requirement	Type of Restart		
		Hot	Warm	Cold
Designation of COOP Site	1. The DOIM will ensure that an alternate site with similar physical configuration is available for back up operations		X	X
	2. The system DAA will ensure the alternate site is ready		X	X
	3. The alternate site will serve as an online spare	X	X	X
DPE Configuration	1. The system DAA and PM will evaluate the DPE configuration at the alternate site to ensure the same performance from an application and a network standpoint.		X	X
	2. The system DAA and PM will ensure that the alternate site will provide the same functional performance		X	X
Facilities, security, supplies, and information transfer	1. The ISSM and ISSO will ensure that the MEDI is made available to the alternate backup site		X	X
	2. The ISSM and system administrator will ensure that similar security and cyber defenses exist at the alternate backup site.		X	X
Personnel requirements	1. Alternate site passwords and accesses will be given to identified personnel from the primary site in the event of a full restart.			X

	2. The alternate site DAA will ensure adequate and trained personnel are available in the event of a move to an alternate site.			X
Planning coordination	1. The DOIM will ensure that the plans for primary and backup sites have been developed and coordinated.		X	X
	2. The system DAA and the ISSM will coordinate in real time with all connected systems during a change from the primary to the backup site.		X	X
Emergency movement procedures	1. The system DAA and the ISSM will determine if and when processing functionality is to be rerouted from the primary to the alternate site			X
	2. Routing tables will be updated when functionality is rerouted from the primary to the alternate site.			X
AUTODIN interface	1. The DOIM will determine if and when AUTODIN functionality is to be rerouted from the primary to the alternate site			X

Contingency Operations as Host Site

site consists of the transfer of operations and control to a backup site. For cyber attacks, the control may not shift from the original site to a backup site. In either event, the following table is applicable.

This section contains the requirements for the host site in the event of a cyber or physical attack. For physical attacks, the contingency planning for the host

Specific Operations Area	Physical Attack	Cyber Attack
Planning coordination	1. The System DAA shall ensure that a contingency plan has been developed. 2. The DOIM shall ensure that contingency planning coordination is maintained for all systems under the DOIM's	1. The System DAA shall ensure that a contingency plan has been developed. 2. The DOIM shall ensure that contingency planning coordination is maintained for all systems under the DOIM's

	control. 3. The ISSM's/ISSO's shall participate in the contingency planning.	control. 3. The ISSM's/ISSO's shall participate in the contingency planning.
Configurations	1. The ISSM shall maintain periodic configuration checks to ensure the accuracy of the information system configuration 2. The ISSM shall immediately (and use automated means if available) verify the configuration and availability of the system on upgrade to increasing INFOCON or DEFCON levels to verify operational readiness and effectiveness of the information system. 3. The ISSM shall inform connected systems and one level up of the configuration state.	1. The ISSM shall maintain periodic configuration checks to ensure the accuracy of the information system configuration 2. The ISSM shall immediately (and use automated means if available) verify the configuration and availability of the system on upgrade to increasing INFOCON or DEFCON levels to verify operational readiness and effectiveness of the information system. 3. The ISSM shall inform connected systems and one level up of the configuration state.
Facilities, security supplies, information transfer, and transportation	1. The ISSM and ISSO will ensure that backup supplies are maintained at the host and contingent sites. 2. The ISSO will ensure the safe transfer of security information and supplies. 3. Op command and PM's will maintain a plan for transportation of critical supplies and personnel between the primary and contingent site. 4. The DOIM, Op command and PM's will maintain a list of responsible backup personnel at the contingent site. 5. The DOIM will decide if and when to release password access information to the responsible backup personnel.	1. The ISSM and ISSO will ensure that backup supplies are maintained at the host and contingent sites. 2. The ISSO will ensure the safe transfer of security information and supplies. 3. Op command and PM's will maintain a plan for transportation of critical supplies and personnel between the primary and contingent site. 4. The DOIM, Op command and PM's will maintain a list of responsible backup personnel at the contingent site. 5. The DOIM will decide if and when to release password access information to the responsible backup personnel.
Personnel requirements	1. The DOIM will maintain a list of personnel who have been designated with password access to systems routers, networks, and other areas of the	1. The DOIM will maintain a list of personnel who have been designated with password access to systems routers, networks, and other areas of

	information system at both the primary and contingent sites. 2. All program managers and ISSM's will maintain a configuration list of areas of the system, both the primary and contingent, where password access is necessary.	the information system at both the primary and contingent sites. 2. All program managers and ISSM's will maintain a configuration list of areas of the system, both the primary and contingent, where password access is necessary.
Billeting and messing requirement	1. Since the location of the contingent site may change as a function of available equipment and network functionality, Op command will periodically ensure that adequate billeting and messing equipment is available at the contingent site.	1. Since the location of the contingent site may change as a function of available equipment and network functionality, Op command will periodically ensure that adequate billeting and messing equipment is available at the contingent site should a cold start at the remote site be necessary.

Evaluation Criteria for COOP and Test Methods

This section contains the requirements for the development of periodic testing for the COOP. Periodic test and analysis is necessary to understand system vulnerabilities and to account for advances in information technologies. The major emphasis on the COOP is its adaptability for maintaining the integrity of the information system.

The DOIM, Op command, and Program Managers will ensure that:

1. Testing of information systems is periodic in nature and all results are recorded
2. Testing of information systems is in accordance with established US Army policy
3. Penetration testing is performed and is in accordance with established US Army policy
4. Testing plans include realistic scenario(s) for a real world cyber attack
5. Testing plans include realistic scenario(s) for a real world physical attack
6. Results of the testing are reported to the DOIM and maintained on a need to know basis.

COOP Requirements for RFPs

This section presents a list of minimal requirements that will be made part of Requests for Proposals (RFPs), Statements of Work (SOWs), and software modifications to new and existing information systems.

Specifically, PEOs and Program Managers shall ensure that requirements are placed on new and modified information systems such that the information system will contain features that:

1. Will prevent unauthorized access
2. Will detect, log, and report all unauthorized access attempts
3. Support positive and unique Id and authentication of individuals and their authorization to system level accesses
4. Protect communications against monitoring and spoofing
5. Guarantees secure interfaces to service providers
6. Implement password mechanisms to restrict access
7. Ensures system level commands are checked for correct syntax and authority
8. Contain tools for the analysis of audit trails
9. Ensures no denial of authorized access.
10. Implement controls to protect information and other soft assets from unauthorized modification
11. Implement controls on the trusted computing base to protect authentication data from unauthorized access, modification, or destruction
12. Automatically prevent virus attacks
13. Provide for security administration of different nodes
14. Implements a set of tools to assist in managing the following security elements:
    a. Security Policy
    b. Users
    c. Information
    d. Information processing systems
    e. Security services
    f. security mechanisms
    g. security functions supporting security mechanisms used to implement services
    h. virus protection

APPENDIX D

FIREWALLS

FIREWALL AND HIGH ASSURANCE GUARD IMPLEMENTATION GUIDANCE

31 December 1998

Table of Contents

Section Page

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This Firewall and High Assurance Implementation Guidance document has been prepared for use by Army

organizations in planning for and implementing firewalls and high assurance guards into their information technology architectures. It is intended to be a guidance document, vice a policy document. The document starts by discussing planning for the implementation of firewalls and is focused on the five firewalls on the Army's firewall blanket purchase agreement (BPA). It presents three tables that an implementer should review. One table lists the protocols that must be permitted through Army firewalls, the second table lists the protocols that may be permitted through Army firewalls, and the third table lists the protocols that should not be permitted through Army firewalls. The main body for the document then closes by presenting guard implementation considerations.

Appendices to this document present more detailed information for assistance in implementing firewalls and guards. Three of the appendices in particular provide detailed guidance to Army organizations implementing either firewalls or guards. Appendix C presents information on the various protocols that a firewall may be required to handle and their security considerations. Appendix D contains a template that may be used in developing an organization's firewall policy. Appendix E contains a template that may be used in developing an organization's guard policy.

Firewall and High Assurance Guard Implementation Guidance

1.0 INTRODUCTION

Paragraph 1 of this document explains the Army program for building security-in-depth for the installation information processing systems. The use of firewalls and guards is introduced in this section. The initial step in this program is to start with the installation boundary and provide firewall-like technology protection between the installation and exterior networks. Paragraph 2 provides information on firewalls. Included in this paragraph is information concerning:

? Firewall technology
? Firewalls on the Army blanket purchase agreements (BPA)
? Additional security measures to build security-in-depth
? Guidance for determining the installation firewall needs
? How to establish a firewall policy
? How to determine which firewall to select
? How to obtain approval for connecting the firewall to the Defense Information Systems Network (DISN).

Paragraph 3 provides information on guards. Included in this paragraph is information concerning:

? Functions of guards
? Guards on the Army BPA
? How to get started with guards
? How to establish a guard security policy
? Guard accreditation and certification

1.1 Purpose

The initial purpose of this document was to describe the Army’s use of commercial

firewalls and guards for the protection of Army installations and the steps necessary to obtain accreditation and certification for connecting these devices to the Unclassified but Sensitive (N) Internet Protocol (IP) Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET). However, between the initial draft and the final version of this document, the Army has decided to build its own initial security protection for Army installations using current firewall technology. This document provides Army-wide implementation guidance that establishes a common set of security practices for installation of firewalls and guards associated with Army fixed installations. The supporting documentation articulated in this document, like the firewall policy describing each Army Post's boundary protection and accreditation package, still need to be written. A firewall provides boundary protection and allows computer network traffic to flow according to rules established in a security policy. Traditionally, the firewall has been viewed as the first element in security-in-depth for the installation's information system. Router filters and intrusion detection devices are often used in front of the firewall to work in combination with the firewall. These devices may be viewed as part of the firewall system. The current Army plan is to provide intrusion detection, firewall-like technology, and a proxy server to protect the initial boundary of each post. Commercial firewalls are still considered useful within each Army post for protecting more sensitive LANs like financial, medical, and personnel. Guards are still viewed as necessary where there is a need to exchange information between the SIPRNET and NIPRNET. A guard provides protection between domains of differing classification and allows traffic to flow according to rules established in a security policy. Figure 1 depicts the firewalls and guards at a notional Army installation and their relationship to the SIPRNET and NIPRNET. This document deals mainly with the SIPRNET and NIPRNET connections to the local Army installation. Other networks that may connect to the Army installation include the Defense Research and Engineering Network (DREN), Medical network, and the Corps of Engineers networks. If any of these other networks are connected to the local domain, then the specific connection needs to be covered by an Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) between designated approving authorities (DAAs) that articulates the operational and security aspects of the connection. Appendix I is a sample MOA/MOU for this purpose.

Figure 1. Firewalls and Guards at a Typical Army Installation

1.2 Background

1.2.1 The Army Firewall and Guard Installation Program. The Department of the Army (DA) has established a program to install firewall technology and

guards at all of the Major Commands (MACOMs) and Army installations. As part of this program, DA will provide for firewall-like boundary protection for NIPRNET and SIPRNET connection at the MACOM and Army Installation level. Should the initial requirement for any of these firewalls terminate, the firewall will revert to DA for reallocation since these firewalls are centrally funded. Based on requirements, a guard will be installed between the NIPRNET and SIPRNET at the locations that have both services.

1.2.2 Passwords. In accordance with DA Message SAIS-PAC-I, Army Wide Network Management, 171653Z Feb 98, passwords are required to be sent to the Army Signal Command for monitoring.

1.2.3 Application to tactical units. While the scope of this document is limited to fixed installations, tactical units that deploy and connect to SIPRNET and NIPRNET are required to have firewall protection for the Army enclave. If these connections are protected by the main post connection then the tactical unit's connection is protected. However, naked connections without benefit of any firewall or intrusion detection exposes those tactical units to avoidable risk. Steps need to be initiated to quantify this firewall requirement in terms of throughput and protocols to be passed. Planning for the use of firewalls to protect tactical systems should be an integral part of contingency planning for deployments. If the situation requires dual routes out of the Army enclave, both routes require firewall protection. A security policy needs to be written to cover the protocols required for these tactical firewalls. Tactical units requiring Secret and Below Interoperability (SABI) will also need to follow the guidance on documentation and installation of guards.

1.2.4 The SABI program. The Joint Staff SABI program requires the installation of guards at certain locations. The aim of this program is to ensure SABI for the warfighter with a level of risk that is deemed acceptable within the community to protect the integrity of and reduce the risk to the Defense Information Infrastructure (DII). Army implementation of this Joint Program identifies places where guards are needed between the secret high networks connected to the SIPRNET and the unclassified networks connected to the NIPRNET. Guidance on security policies, certification, and accreditation is provided in this document.

1.3 Responsibilities

This section describes the personnel who must carry out this guidance and the specific responsibilities ascribed to each.

1.3.1 MACOM/Installation Commander. Each MACOM and Installation Commander is responsible for the following:

? Establish a security policy covering the installation of the firewall connection to the NIPRNET. Guidance for doing this is included in the remainder of this document. This policy

must address the needs of all Army and non-Army tenant organizations on the post such as hospitals, Red Cross, National Park Service, Department of Interior, Drug Enforcement Agency, and National Guard/Army Reserve.

? Provide the Communications Security Logistics Activity (CSLA) with a purchase request for any additional firewalls to be installed on post that are needed to support the security-in-depth concept. See DA Message, Army Approved ISS Products, 170835Z Jun 98.

? Prepare the Certification and Accreditation package for the firewalls following DoD Information Technology Security Certification and Accreditation Process (DITSCAP) procedures as discussed in this document. Guidance is provided in appendix G and H of this document.

? Provide the associated passwords to the Army Signal Command (ASC) for monitoring purposes per the requirements of DA Message SAIS-PAC-I, Army Wide Network Management, 171653Z Feb 98.

1.3.2 DISC4. DISC4 is responsible for the Sustaining Base Security Policy Establishment, Promulgation, and Enforcement.

1.3.3 MACOMs. The MACOMS are responsible for:

? Enforcing DA policy to include appointment of an Information Systems Security Program Manager (ISSPM) see AR 380-19.

? Establishing a MACOM security policy.
? Reporting to DA on compliance with policy.
? Developing MACOM systems using the Network and System Management Configuration Control Board (NSM CCB) managed protocols.
? Reporting of new sustaining base interoperability parameters to the NSM CCB.

1.3.4 The Information Systems Security Program Manager (ISSPM). AR 380-19 requires appointment of an ISSPM at each Army MACOM and within the Office of the Administrative Assistant to the Secretary of the Army. The ISSPM will perform duties as prescribed in paragraph 1.6.d.(1) of AR 380-19 including, among others the following related to firewalls and guards:

? Establish and mange the command Information Systems Security (ISS) program
? Promulgate ISS guidance within each command, to include developing command-unique guidance for firewalls and guards.
? Establish a procedure within the command to document the status of all AIS accreditation to include firewalls and guards as appropriate.
? Oversee the training program to ensure the System Administrators are trained on the firewalls and guards.
? Developing and administering an Internet policy.
? Ensure that each AIS under security supervision has adequate security documentation.

1.3.5 CSLA. The CSLA will provide logistics support and maintain the Army BPA on firewalls and guards.

1.3.6 NSM CCB. ASC, USAISEC, and Program Executive Office (PEO) Standard Army Management Information System (STAMIS) created the NSM CCB in 1994 to establish and maintain a standard Network and System Management (NSM) solution supporting the sustaining base.

1.3.7 Army Computer Emergency Response Team (ACERT). The ACERT will coordinate responses to intrusions/attacks noticed by firewalls or firewall administrators.

1.3.8 The Army Network and Systems Operation Center (ANSOC). The ANSOC will:

? Provide Maintenance of DA minimum Firewall rule sets on installation gateway firewalls.
? Serve as member of NSM CCB.

1.3.9 Program Executive Officers (PEOs)/Program Managers (PMs): The PEOs and PMs will:

? Develop systems using the NSM CCB managed protocols.
? Report new sustaining base interoperability parameters to the NSM CCB.

1.3.10 Installations and their tenants. The various installations and their tenants will:

? Reinforce the one Director of Information Management (DOIM) concept.
? Require tenants to coordinate/get all off-post services through the installation DOIM.
? Identify the protocols required to be passed for current transactions to the DOIM.
? Coordinate unique security requirements DOIM.
? Notify NSM CCB of deviations to standard configuration.
? Provide properly trained personnel to maintain/operate the firewall.

1.3.11 Firewall/Systems administrator. The Firewall Administrator will be a systems administrator (SA) with special training in firewalls and will:

? Maintain minimum educational requirements as prescribed by the specific firewall selected.
? Ensure the operating system for the firewall is configured properly and that the security features are properly set according to the security policy.
? Use approved C2 protect tools to periodically review firewall security.
? Periodically check with the firewall manufacturer to keep informed of firewall security problems and patches as they are developed and apply them as appropriate in order to maintain firewall security.
? Ensure audit software is properly configured and audit trail reports are periodically reviewed in accordance with the command's firewall policy and AR 380-19.
? If a SA suspects an unauthorized user is attempting to access the AIS, the SA is authorized to take the actions necessary to verify and limit the penetration attempt from an unauthorized user. Once

verified, the SA will notify, concurrently, the chain of command and contact their supporting CERT. The appropriate individual within the chain of command will notify Counter Intelligence (CI) and Criminal Investigation Division (CID). The SA may make system backups of appropriate log, history files and user directories. Once the SA has determined that the anomaly is in fact an unauthorized intrusion, and CI and CID have been notified, the SA will not in any other manner specifically target, track or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation.
? Comply with Army procedures for Information Assurance Vulnerability Alert (IAVA). Briefly, these procedures require the SA, when notified, to access the DISA IAVA web site to review the alert information, assess the local impact, fix vulnerabilities, and/or request waiver from the DAA and report back through chain of command on actions taken.

2.0 FIREWALLS

This section describes the firewall, its role in security-in-depth, and its associated technologies. The conclusion of this section contains a discussion of the firewalls on the Army Blanket Purchase Order Agreement (BPA) and the protocols they support.

2.1 Definition

Put simply, a firewall is a mechanism to protect a trusted network from an untrusted network. Typically, the two networks in question are an organization's internal (trusted) network and the (untrusted) Internet; however, in the Army context, a firewall is installed between the Army installation and the DISN for both the SIPRNET and NIPRNET as depicted in figure 1. Physically, a firewall controls access to one or more host systems and routers and incorporates other security measures.

2.2 Purpose

This Army program will establish boundary protection for all Army installations. This boundary protection is the first step in forming security-in-depth to protect the information systems on Army installations. Other measures need to be taken to build security-in-depth. A notional security-in-depth is depicted in Figure 2. While this is not officially sanctioned DA architecture, it is used as an example of security-in-depth. In this notional system, additional security measures are taken in terms of hardware, software, and procedures to enhance the protection provided by the firewall.

2.2.1 Additional hardware. Additional hardware includes the establishment of a demilitarized zone (DMZ) where web servers and other publication servers are placed for the public to access. The purpose of the DMZ is to isolate the organization's few servers that service the Internet from the many servers and machines that service the rest of the organization. For example, an e-mail screening server is placed on this DMZ to detect threats and embedded malicious

code. Other application-unique servers may be placed on this DMZ to offload the firewall processing as needed. Intrusion detection systems funded by DISC4 have been installed initially on each post's access path. Additional intrusion detection systems funded by the posts may be required on internal servers and enclaves to support the security-in-depth concept. Each network segment needs to be evaluated separately for such systems to monitor and detect unwanted activities. Security logs are maintained on an internal server separate from the firewall. The firewall acts as a domain name server (DNS) proxy for the external network while an internal server provides this function for the internal network. This limits the amount of information available to the external network. Sensitive information (such as financial or medical information) may be placed behind an internal firewall as needed.

Figure 2. Notional Security-in-depth

2.2.2 Additional security software. The IDS hardware devices have intrusion detection software to detect unauthorized intruders on each of the network segments. Additional intrusion detection software includes software residing on the firewall and on key servers on the internal network. Key servers include the DNS, mail servers, and any other server deemed sufficiently sensitive to warrant this protection.

2.2.3 Additional procedures. Additional procedures include periodic security scans on the firewall from the external network, on the DMZ from a DMZ connection, and on the internal network from an internal connection. Additionally, these scans should be made when changes are made to the network to verify that the security posture has not been compromised.

2.3 Firewall Technology

Firewall technology is continuously evolving. The first firewalls were simple filters implemented using router technology. The second generation of firewalls implemented application gateways, sometimes called proxies, which isolated the application from the LAN being protected. Third generation firewalls include both stateful filters and dynamic detection. Security enhancements are also available which strengthen the firewall protection. This section discusses each of these technologies, as well as firewall security enhancements.

2.3.1 Packet filtering. The simplest form of a firewall is a router configured to screen the packets entering your network. This is referred to as router-based security and is an integral part of all firewalls. The router can be programmed to accept or deny access based on source and destination addresses as well as on the protocol being transported. It is also known as a screening router or packet filter. The information this tool acts on is contained in the transport layer and the network layer of

the seven layer Open Systems Interconnection (OSI) Model (see Figure 3). The packet filtering firewall is not as effective as the application gateway firewall in securing network traffic because the information it acts on is limited. These filtering firewalls generally have the highest performance in terms of speed; however, applications are allowed through the firewall to operate directly on the user's workstation. No protection is provided against damage from innocent bad code that is passed through or against intentionally generated bad code passed to create disruptions.

Figure 3. Firewalls and the OSI Model

2.3.2 Proxies. The terms "proxy" and "application gateway" mean the same thing. In a firewall, a proxy is a software mechanism that acts on behalf of another. It will sit between a client on one side of the firewall and a server on the other. To the client it looks and acts like a server; to the server it looks like client software. It acts as a proxy for both sides. The important feature is that there is no direct connection to the internal user/server. It protects the internal machines that may be susceptible to hackers simply because they have not been hardened or because they do not have current software upgrades installed. Gateways or application gateways can handle store-and-forward traffic as well as some interactive traffic. Application gateways are programmed to understand the traffic at the user application level, layer 7 of the OSI Model. Access controls can be provided at the user level and application protocol level. An intelligent log of all usage of that application can also be maintained. The ability to log and control all incoming and outgoing traffic is one of the main advantages of having an application-level gateway. The gateways themselves can have additional security built into them as needed. A disadvantage of application-level gateways is that a custom program has to be written for each application. The custom application program acts as a proxy that accepts incoming calls and checks them against an access list of what types of requests are permitted. Most proxies for applications like File Transfer Protocol (FTP), Telecommunications Network (TELNET), and Hypertext Transfer Protocol (HTTP) are available commercially. Servers on which these applications reside are known as proxy servers.

2.3.3 Stateful inspection. Stateful inspection is a technique for packet filtering that overcomes most of the weaknesses inherent in using router filters (described in paragraph 2.3.1). The stateful inspection module is loaded into the operating system at a point in the Internet Protocol (IP) stack where it can preview packets before they reach the Internet layer where routing takes place (between layers 2 and 3). At this point, the product resembles packet filtering. However, stateful inspection may examine the information in layers 3 through 7 and keep track of past history. While the stateful

inspection machine does not participate in the application session as a proxy does, it is cognizant of what is happening at the application layer. When the first packet representing a new transaction is received, a rules base is used for deciding to permit or deny the packet and the packet is stored as state information. Subsequent packets can then be permitted or denied based upon the current state, instead of the rule-based decision-making process. Also, examination of the data within the packets is permitted; thus, rules can be assigned based on that data. Dynamic detection uses the stateful inspection techniques. The stateful inspection firewall can be programmed to detect hacker attacks much like intrusion detection products do. Thus, known hacking signatures can be programmed into the firewall. Scripting is generally available to write custom routines. Few routines are available commercially. Stateful inspection allows direct connection to users/servers in the protected zone. Configuration of this type of firewall is more complex than the configuration of the pure proxy firewalls.

2.3.4 Proxy versus stateful inspection. There is a lively ongoing debate within the security community regarding the strength of the security provided by stateful inspection compared to the security provided by the proxy. The strength of the proxy server is that all transactions take place on the proxy. Note that the proxy firewall does not allow a direct connection between internal and external networks. Therefore, only the proxy server needs to be fortified against attack. Proxy technology has proven itself to security managers. They know and trust this product; however, when looking at throughput, the proxy appears to constrain the throughput when compared to the stateful inspection machine because the proxy must process the transaction and relay it to the user machine.

Acting like a router, the stateful inspection server examines each packet and allows or denies the transaction to pass to the user's machine according to the packet's configuration. Security managers are uneasy about this because the transaction is passed on to a machine on the internal network, and they are concerned about having to fortify each machine in their network. Because stateful inspection is a new technology, it has not withstood rigorous field use and has not earned a reputation over time like the proxy server has. Therefore, it is viewed with less comfort by much of the Information Security (INFOSEC) community. Also, although stateful inspection is generally considered to have a higher throughput than the proxy machine because it routes/filters the information, some research indicates otherwise. An article in the March 21, 1997, edition of Data Communications magazine entitled, "Firewalls: Don't Get Burned," indicates that the throughput performance of a stateful machine drops off earlier than some of the other proxy-based firewalls.

2.3.5 Firewall security enhancements. There are a number of add-ons to firewalls that enhance the total security posture. Authentication devices, intrusion detection, and encryption supporting virtual private networking are among the more popular enhancements.

(1) Authentication devices. Authentication devices apply technology to strengthen the authenticating process. Some organizations use SecurID authentication, which strengthens this process by requiring the user to enter a number that is generated by the user's SecurID card. This number changes in a manner known to the authentication server and thus uniquely identifies the individual to the system. An authentication system based on digital signature like the FORTEZZA card from the Multilevel Information System Security Initiative (MISSI) program, would be stronger but also more costly.

(2) Intrusion detection. There are two types of intrusion detection systems, those that protect a server and those that protect a network. An integrated security-in-depth requires both types. Like firewalls, the intrusion detection systems become vulnerable to new hacker techniques. Intrusion detection devices must be capable of being updated with the latest detection software to keep pace with the evolution of the technologies available to the hacking community.

(3) Virtual private network (VPN) products. VPN techniques are relatively new and only a few firewalls support them. VPNs are established between firewalls to form a many-to-many relationship between LANs or from a single PC to the firewall to form a one-user-to-LAN relationship. The links established are encrypted and various encryption packages are supported.

2.4 Firewalls on the Army Blanket Purchase Agreement (BPA)

There are five firewalls on the Army BPA:

? Raptor, manufactured by AXENT Technologies, Inc., with a choice of the following Operating System (OS): HP-UX, Solaris, and WinNT.
? Gauntlet, manufactured by Network Associates, with a choice of the following OS: Solaris, HP-UX, and WinNT.
? SmartWall, manufactured by V-ONE Corp. with a choice of the following OS: BSDI, HP-UX, Solaris, and WinNT.
? Sidewinder, manufactured by Secure Computing Corporation (SCC), with Berkley Software Design, Inc (BSDI) OS.
? Sunscreen SPF 200, manufactured by Sun Microsystems, with Solaris OS.

While these firewalls are available with different operating systems, it should be noted that Defense Message System (DMS)-compatible firewalls are available from V-ONE on a HP/UX or Berkeley Software Design, Inc. (BSDI) platform and from Secure Computing Corporation's (SCC) Sidewinder on a BSDI platform. The following paragraphs describe

these five firewalls. The description of the Eagle firewall is taken from the Raptor Systems' web page at raptor.com. The description of the other three firewalls comes from the web page of the National Security Agency's (NSA's) X3 testing division. The description of Sunscreen SPF 200 was taken from Sun's web page at sun.com.

2.4.1 Raptor (Eagle). Note: With the merger of Raptor Systems with AXTENT Technologies, the Raptor product names will migrate from the Eagle name to the Raptor name to be consistent with AXTENT's product naming convention. Raptor Systems' Raptor NT 6.0 firewall and Raptor Firewall 6.0 for Solaris are enterprise security products that offer the proven security of application-level proxies, combined with the flexibility and extensibility of packet filtering. Both versions incorporate the broadest range of security features, including secure tunneling with IPSec and ISAKMP/Oakley industry-standard protocols, IP spoof checking, a wide selection of strong authentication alternatives, a powerful and flexible management interface, and the industry's only firewall-integrated content blockers, WebNOT and NewsNOT. Introduced in early 1996, EagleNT was the first Microsoft Windows NT-based firewall on the market. Today, RaptorNT is the only NT-based firewall in its third generation. EagleNT offers tight integration with Windows NT services and authentication capabilities. This integration, plus the implementation of high performance, multi-threaded services and a simple management interface, make EagleNT the most secure, manageable, and flexible solution for your enterprise Internet security needs.

2.4.2 Gauntlet. Network Associates' Gauntlet version 3.0 firewall is an application gateway firewall. The Gauntlet firewall is implemented with a conservative design philosophy, acting as a complete traffic block and transporting all traffic through application layer proxies that gateway each service on behalf of the user. Gauntlet 3.0 also supports transparent proxies, strong authentication capabilities on several of its proxies, and virtual private networking with other Gauntlet firewalls. Gauntlet firewalls provide detailed traffic reports and a complete audit trail for information passing the firewall.

2.4.3 V-ONE SmartWall. The V-ONE SmartWall version 3.3.1 with SmartGate 2.1.1 is an application gateway style firewall with an IP screening utility that can be configured to allow the passage of protocols for which there is not a specific application proxy. The SmartWall also provides strong authentication capabilities on several of its proxies and virtual private networking with other V-ONE SmartWall firewalls. Also, the SmartWall has a feature called SmartGate that allows clients to securely connect to the firewall using both strong authentication and encryption. The V-ONE SmartWall version 3.3.1 product includes the Network Associates' Gauntlet kernel 3.1, in addition to

the SmartGate version 2.1.1. Both were analyzed in the NSA testing. SmartWall is available on both the Gauntlet and the Raptor firewalls.

2.4.3 Sidewinder. The SCC Sidewinder firewall V4.0 product is an application gateway style firewall that is designed to protect an organization's internal network while providing a connection to an external network. The major feature that distinguishes the Sidewinder from other firewalls is the addition of Type Enforcement (TE) technology. The TE is implemented at the UNIX kernel level and controls what users can do on the system and which files a specific process running on the system can access. The system is divided into domains, each of which has access to only those resources that are needed to perform their function. Type Enforcement also assigns a file type to various groups of files that restricts access to those groups on the basis of their types. The Sidewinder uses roles to restrict a user's access to domains. The V2.12 product adds additional capabilities over the previous version tested (V1.0) by the X31 firewalls group. Among these is the addition of a FORTEZZA capability. FORTEZZA provides strong identification and authentication for users who need to TELNET or FTP from their workstations. This version also adds additional services like NNTP, TELNET, support for generic proxies, and support for unsecured Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

2.4.4 SunScreen SPF 200. The SunScreen SPF package is Sun's strategic platform for perimeter defense, providing secure business operations over the Internet. To ensure a high level of security, SunScreen SPF uses a stealth design to protect it from attack and state-of-the-art Simple Key Internet Protocol (SKIP) encryption to protect data going over the network. Its advanced dynamic packet filtering, coupled with Sun's high-speed hardware, is designed to meet the most demanding performance requirements. The SunScreen SPF solution enables organizations to deploy a premier perimeter defense today and accommodate business over the Internet at their own rate in the future. SunScreen ESF was rated the fastest firewall in a recent Data Communications performance test (March 21, 1997) that included the top firewall vendors. Given SunScreen SPF's internal design and optimization, SunScreen SPF should run even faster. SunScreen SPF performance ensures that it can keep up with the demands required to screen large amounts of Internet traffic. The stealth design, which makes SunScreen SPF not addressable with an IP address, provides two benefits. First, stealthing makes a SunScreen SPF system more secure because potential intruders cannot address the machine running SunScreen SPF, possibly compromising the machine. Second, installation of SunScreen SPF into the network is easy since the administrator can install it without changing tables. The stealth design "hardens" the OS and turns the system into a dedicated

SunScreen. SPF system only runs SunScreen SPF. Hardening the OS enhances security. Since other applications do not run on the system, there is less exposure. SunScreen SPF uses a separate administration station that can be any SPARC machine and need not be dedicated. State-of-the-art SKIP encryption technology provides secure network communication and acts as the infrastructure for electronic commerce, extranets, and secure remote access. SKIP protects the data being transmitted, ensures its integrity (not altered), and provides a high level of authentication. SunScreen SPF covers both TCP and UDP services. In regards to UDP, SunScreen SPF maintains state to improve performance and SunScreen SPF allows flexibility in logging what has passed or failed through the screen. Administrators can choose what they want to monitor and be alerted to problems through pagers or alerts to management. To provide additional protection for the internal network Network Address Translation (NAT), SunScreen converts internal addresses to a different set of public addresses which also helps those sites that have not registered their IP addresses. NAT supports both static and translation of internal addresses to public addresses. Since hackers do not know the internal hosts' addresses, attacks are minimized. Administration is done through secured, remote administration stations, enhancing security and meeting the needs of organizations for remote management.

2.5 Getting Started with Firewalls

Two sets of documentation are required to support the installation of the firewall. One is to support the connection to the DISN; the other is to support the requirements of DOD 5200. The documentation for both is almost identical.

2.5.1 DISN connection documentation. This section is written with the assumption that a prior certification and accreditation package exists for the installation's connection to the DISN. This package only needs to be updated with the firewall information and re-certified. If the accreditation package does not exist, one has to be created following the guidance in appendix G. To receive approval to connect to the DISN (SIPRNET and NIPRNET), the Defense Information Systems Agency (DISA) requires the information and documentation listed in Table 1.

Table 1. Documents needed for DISN connection

1 A Letter of Accreditation or Interim Authority to Operate (from the SSAA see paragraph 2.5.2)
2 An installation system connectivity diagram
3 A consent to monitor statement
4 A statement of significant or residual risk
5 Non-DOD connections (e.g., contractor, foreign, etc.)
6 A statement of minimal security requirements as stated in the accreditation plan
7 A statement of specific security features and implementations, such as firewalls, guards, and secure network servers, as stated in the security concept of

operations
8 Copies of any memorandums of agreement/understanding (MOA/MOU) with any other interconnected systems or networks
9 The mode of operation
10 The maximum level of sensitivity of information processed

2.5.2 DITSCAP documentation. Under Department of Defense (DOD) 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997, each installation is required to maintain a System Security Authorization Agreement (SSAA), which includes much of the information required for connection to the DISN. Appendix H contains an outline of the SSAA document.

2.5.3 Firewall location. From the connectivity diagram (item 2 in Table1), determine an appropriate physical location for the firewall. Keep in mind the physical security requirements that only the system's administrators and information security personnel should access the firewall. If the firewall is on the SIPRNET, it must be in an approved secret secure area. Backup power is required for the firewall if installation facilities are required to operate during primary power outages. There should be MOA/MOUs (item 8 of Table 1) that describe the security operating conditions of all the installation networks being protected by the installation firewall. These need to be current; from them one can determine if there are any back doors via modems or other Internet connections that could provide unauthorized/unmonitored access to the installation's network. Also, from these MOAs/MOUs, it can be determined if additional firewalls are required behind the installation firewall to isolate Sensitive but Unclassified (SBU) networks containing financial, medical, Freedom of Information Act (FOIA), or other sensitive data from the remainder of the installation.

2.6 Protocol Determination

The next step is to determine the protocols that are required to pass through the firewall. There are three methods for determining these protocols; at least two should be used for verification.

2.6.1 First method. The first method is to use a protocol analyzer with a data reduction tool (an intrusion detection device may be substituted for this purpose) on the external installation connection and record all protocols for a period of one month to catch monthly activities. (This has to be done for both the SIPRNET and the NIPRNET.)

2.6.2 Second Method. The second method is to visit every organizational user on the installation and determine what protocols they are currently using for transactions over the DISN for both the SIPRNET and NIPRNET. Make sure all tenant organizations are included. Appendix F contains a partial listing of the protocols associated with STAMIS programs. This listing will

become valuable for determining Army wide protocols once a complete listing is obtained. This second method is valuable in determining if there are other Internet connections behind the installation firewall. Some of the post tenants do business on the Internet and may have their own direct connections; for example, hospitals have links to laboratories. If there are other outside connections, security measures need to be taken to mitigate the risk. An internal firewall might be appropriate. The installation survey should also determine projected use of any emerging protocols for video and audio.

2.6.3 Third method. The third method is to select from the following protocol lists based on their importance and function. All of the potential protocols that could be associated with the firewall functions are listed in this section and detailed in Appendix C. The protocols have been placed into three lists: must/should allow, may desire to allow, and should block.

(a) Must/should allow. The protocols listed in Table 2 are the protocols that are necessary to support Army-wide business transactions of the installation.

Table 2. Protocols to be Used
Protocol Function Recommendation
DNS Domain Name Services Allow one-way, inside-out, use split DNS servers.
epmp, port 135 End point map Allow one-way, inside-out.
IP Internet Protocol Drop packets arriving on outside addressed to inside.
IPX Internet Packet Exchange If used on a site, allow IPX traffic through the firewall.
iso-tsap International Standards Operation_Transport Layer Service Access Protocol Allow through the firewall. Outbound packets reflect firewall address.
MIME E-mail extension Permit through firewall.
POP3 Post Office Protocol Use only through a Proxy.
SMTP Used for e-mail Allow only through a proxy port 25.
TACACS, port 49 Terminal access controller, access control system Allow through the firewall for restricted users.

(b) May desire to allow. The protocols listed in Table 3 are the optional protocols that may be necessary to support installation-specific business transactions.

Table 3. Protocols that May be Used
Protocol Function Recommendation
CMIP, ports 163 and 164 Management Protocol Allow through, enable authentication, access control, and logging features
Echo, port 7 Network management Allow outbound requests, allow inbound responses.
FTP, ports 20 and 21 File Transfer Protocol Allow all outbound, deny inbound. Allow if VPN is used.
Finger, port 79 Used to locate other users Allow all outbound, block incoming, respond with security banner.
Gopher, port 70 Used to find text base files on the Internet Allow outbound only, use only with the SOCKS proxy.

HTTP, ports 1023 and 80 Used to search information on web servers Allow outgoing HTTP; incoming HTTP directed to web servers placed on a DMZ.
ICMP A control management protocol Block incoming ICMP messages, do not respond back.
RPC, port 530 Used as a transport protocol for NFS and NIS Allow outbound only, block incoming.
SET Used to encrypt transmissions Allow use as required through port 227.
S-HTTP, port 443 Used to encrypt HTTP Allow use as required.
S-MIME Secure mail extension Allow use as required.
SSL, port 443 Secure socket layer adds security features to enabled applications Allow use as required.
TELNET Used for remote computing Allow only through a proxy; allow only outbound sessions through port 23.
UDP User datagram protocol Allow through.
VPN Virtual private network Allow to known users, must have identical firewalls.
Whois Command port 43 Network information Allow outbound, block inbound use.

(c) Should block. The protocols listed in Table 4 are the protocols that expose the installation to unwarranted security risks and should not be allowed through the firewall and should, therefore, be blocked.

Table 4. Protocols that Should Not be Used.
Protocol Function Recommendation
Archie Index Search of FTP Servers Block port 1525.
EGP Exterior gateway protocol Block use.
IRC port 194 Allows chat between two users Block use.
NetBIOS, ports 137-139 Used for LAN communications Do not use for WAN; block ports 137, 138, and 139.
NFS, port 2049 Used for a network file system in Sun Microsystems network Do not use; block port 2049.
NIS Network Information Service Block use.
NNTP, port 119 Used to transfer network news across the network Do no use, block port 119.
NTP, port 123 Used to synchronize time between computers Do not use; block port 123.
OSPF Open Shortest Path First Block.
Open Windows, port 2000 Used by Sun Systems for GUI Do not use; block.
r-commands Used for remote computing Block all r-commands ports 513 and 514.
RAP Distributes routing information Block RAP port 38.
RIP Determines paths through the network Block RIP port 520.
SNMP Used to manage the network Block port 161 and allow port 162 only if alarms need to be monitored from outside the network.
TFTP Trivial file transfers Block TFTP port 69.
UUCP Older UNIX file transfer protocol Block UUCP port 540.
Whois Used to look up information on users Block port 43.
WAIS Information service like Archie Block port 210.
X-Window A networking windowing system Do not allow;

Block ports 6000 – 6063.

2.7 Firewall Security Policy

A firewall security policy describes how the firewall is to be configured and operated. This information is a matter of record and is the basis of understanding among the installation commander, the Designated Approval Authority (DAA), the firewall administrator, and the information systems security officer for how the firewall is to function. Once an understanding has been reached regarding the protocols to be allowed into and out of the installation, then writing a security policy for the firewall is a simple task. A sample generic policy is included in Appendix D. Guidelines are provided below:

(a) A fundamental policy statement is to disallow everything not expressly allowed. This should be the first statement in the policy.

(b) Some operations, such as the transfer of a large database, slow down the network for other users. These transactions may be restricted to a certain time-of-day use and to a specific set of users.

(c) The security policy should state what protocols are to be audited.

(d) The security policy should state what protocols that have been associated with vulnerabilities may be used if VPNs are in use between compatible firewalls.

(e) There should be a statement on the separation of administrative and security functions. One of the security functions is to review the firewall logs.

(f) The policy should state what, if any, virus checking functions of the firewall are to be enabled.

(g) The policy should address the authentication mechanism enabled. Use of Windows NT Domain and Gateway Authentication models should be restricted. Only authorized models should be used, i.e., ACE, S/key, and FORTEZZA Cards.

(h) A statement of how firewall passwords will be controlled and changed should also be included. All factory passwords should be removed.

2.8 Selection of An Appropriate Firewall

Once the policy the firewall is supposed to enforce has been articulated, then a firewall on the Army BPA can be selected. This should be accomplished by forming a matrix of what is needed for the installation versus the capabilities of the five BPA firewalls. The firewall best suited to meet the user's mission requirements should be selected.

2.9 Ordering the Firewall

When funding is available, the firewall will be ordered through CSLA. The point of contact (POC) is Julia Conyers-Lucero, DSN 879-8259, commercial (520) 538-8259, e-mail luceroj@huachuca-emh1.army.mil.

2.10 Re-certification

The firewall connection to the DISN will require re-certification

prior to activation of the firewall. This re-certification process is described in Appendix G.

2.11 Operation and Maintenance

The local installation organization will be responsible for the operation and maintenance of the installed firewall. This includes administration, periodic security scans to verify the security functionality of the firewall has not changed, and analysis of the firewall security logs.

2.12 Upgrades

After installation, any changes to the firewall will have to be made in accordance with the accreditation process.

3.0 GUARDS

This section describes the guards and their role in a gateway between two networks and will relate to the DOD SABI program requirements. That description is followed by a discussion of the technologies associated with guards. This section ends with a discussion of the guards that are currently available.

3.1 Definition of a Guard

A guard is a trusted processor that protects a system high network from a network of a lower classification and allows the higher-level network to exchange messages with the lower level network under a predefined security policy statement.

3.2 Purpose

“The SABI vision is to ensure secure secret and below interoperability for the warfighter within community acceptable risk to protect the integrity of and reduce the risk to the defense information infrastructure.” This vision statement was taken from the SABI Handbook dated 22 September 1997. The DA has interpreted this to mean that every installation that has both a SIPRNET and NIPRNET connection will also require a high assurance guard to interconnect the two networks.

3.3 Functions of the Guards

Guards are used to enforce a security policy that defines acceptable transactions between two networks operating at different sensitivity levels. Guards are being implemented to automate the downgrading function and relieve the load on the operator in the middle making the downgrade decision. If the downgrading policy has a specific rule set to follow, and the guard can be configured to enforce that policy, then the man in the middle is no longer required. The actions of the guard are very simple, pass the traffic if the rules are followed. Do not pass the traffic if the rules are not followed. When the rules are not followed the guard will pass the traffic to the security officer. The guard may be configured to audit all transactions, transactions only in one direction, or only those transactions failing the policy checks. The guard is trusted to make reliable checks on things such as:

(a) Format Checking. This can be as simple as not allowing attachments to e-mail to flow. It can also be used to check for security labeling like “unclassified” or “secret” in the beginning of the message and

for paragraph markings of (U) and (S).

(b) Dirty word checking. Words such as “secret” or “top secret” in the body of the message or other combinations of words that have classified meanings when used in combination. The guard can check for these and disallow the message based upon the written security policy.

(c) Context checking. These filters are much harder to configure but may also be needed. These filters can identify the use of particular terms in particular contexts. For example, a phrase or code word might have a classified implication when used with a particular country.

3.4 Guards on the Army BPA

Only the Wang XTS 300 High Assurance Guard (HAG) is currently on the Army BPA. The XTS-300 is a general-purpose high assurance guard that can be tailored for many applications. It is evaluated at class B-3 or above. The DMS program has developed the DMS Guard using the XTS-300. As of the 1st quarter FY 99, the WANG HAG will be known as the DII Guard; it will be able to process both DMS and SMTP traffic. This guard is a hardware/software suite that will provide connectivity between Secret DMS enclaves and SBU DMS enclaves. It allows information to flow bi-directionally between the two enclaves if and only if the information first passes a series of checks based on a site enforcement policy. Information that fails such security checks will not be allowed to pass through. The Secure Network Server (SNS) is a legacy guard and may still be operating in some areas.

3.5 Getting Started with Guards

The process in this section closely parallels the process discussed in Section 2.3, Getting started with firewalls. This is because the certification and accreditation process requires the same documentation. This section assumes that a prior certification and accreditation package exists for the installation’s connection to the DISN; this package only needs to be updated with the guard information and re-certified. A general principle for positioning guards is that they should service a limited number of users and be physically located close to them.

3.5.1 DISN connection documentation. This section is written with the assumption that a prior certification and accreditation package exists for the installation’s connection to the DISN. This package only needs to be updated with the guard information and re-certified. In the case where the accreditation package does not exist, then one has to be created rather than updated following the guidance in Appendix G. To receive approval to connect to the DISN (SIPRNET and NIPRNET), the Defense Information Systems Agency (DISA) requires the following information and documentation listed in Table 5.

Table 5. Documents Needed for DISN Connection

1 A Letter of Accreditation or

Interim Authority to Operate (from the SSAA see paragraph 2.5.2)
2 A connectivity diagram for the guard installation
3 A Consent to Monitor statement
4 A statement of significant or residual risk
5 Non-DOD connections (e.g., contractor, foreign, etc.)
6 A statement of minimal security requirements as stated in the accreditation plan
7 A statement of specific security features and implementations, such as firewalls, guards, and secure network servers, as stated in the security concept of operations
8 Copies of any memorandums of agreement/understanding (MOA/MOU) with any other interconnected systems or networks
9 The mode of operation
10 The maximum level of sensitivity of information processed

3.5.2 DITSCAP documentation. Under Department of Defense (DOD) 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997, each installation is required to maintain a System Security Authorization Agreement (SSAA), which includes much of the information required for connection to the DISN. Appendix H contains an outline of the SSAA document.

From the connectivity diagram (item 2 in table5), determine an appropriate physical location for the guard. Keep in mind the physical security requirements that only the system's administrators and information security personnel should have access to the guard. If the guard is on the SIPRNET, it must be in an approved secret secure area. Backup power is required for the guard if installation facilities are required to operate during primary power outages. There should be MOA/MOUs (item 8 of Table 5) that describe the security operating conditions of all the installation networks being protected by the installation guard. This needs to be current; for from them one can determine if there are any back doors via modems or other Internet connections that could provide unauthorized/unmonitored access to the installation's network.

3.6 Guard Purpose

The only reason to require a guard is to permit the bi-directional flow of e-mail or (DMS) messages. This traffic may be permitted with or without attachments according to the policy being implemented. Other functionality, such as database transfers, require additional tailoring and security evaluation. Generally, the flow from a high to a low system is considered a downgrade and needs to be audited. The identity of the individual performing the downgrade must be included in the audit, thus the need for the FORTEZZA card and digital signature. The flow from low to high is not as critical, but also requires some scrutiny to protect against virus and malicious code transmission.

3.7 The Guard Security Policy

Writing a security policy for your guard is somewhat easier than for a firewall because there are not as many protocols to be concerned with. However, the principles remain the same. Once an understanding has been reached of what the guard is suppose to do, then writing a security policy is a simple task. A sample generic guard policy is included in appendix E.

(a) The policy should disallow everything not expressly allowed.

(b) The policy may restrict use to a particular time-of-day or a particular set of users.

(c) The policy should specify what is to be audited and how the security logs are to be processed.

(d) The policy should specify separation of administrative and security functions.

(e) The policy should specify what virus checking functions should be performed by the guard.

(f) The policy should specify how digital signature from the FORTEZZA card is to be used to verify permissions of persons allowed to downgrade.

(g) The policy should specify that all factory passwords be removed from the guard.

3.8 Guard Selection

The Army will offer only the WANG DII Guard on a BPA. This is the only HAG that NSA is going to offer.

3.9 Ordering the Guard

When funding is available, the guard may be ordered through CSLA. POC is Julia Conyers-Lucero, DSN 879-8259, commercial (520) 538-8259, E-mail luceroj@huachuca-emh1.army.mil.

3.10 Operation and Maintenance

The local installation organization will be responsible for the operation and maintenance of the installed HAG. These responsibilities include administration, periodic security scans to verify the security functionality of the HAG has not changed, and the analysis of the HAG security logs.

Appendix A, REFERENCES

The following sources were consulted in preparing this guidance document.

A.1. Government Documents

Army C2 Protect Program Management Plan (PMP).

Army Regulation 380-19, Information Systems Security, February 27, 1998.

DA Message, SAIS-PAC-I, Army Wide Network Management, 171653Z Feb 98.

Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), Deploying Firewalls in a DII COE Environment Running Distributed Computing Environment (DCE) and Common Desktop Environment (CDE), October 22, 1996.

Defense Information Systems Agency, DISN Connection Security Requirements, Final Draft, November 1997.

Defense Information Systems Agency, Defense Message System Product Compliancy Handbook (interim Draft Release 1.2), August 1996.

Department of Commerce, Internet Security Policy: A Technical Guide (DRAFT), NIST Special Publication 800-XX, (undated).

Department of Commerce, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls, NIST Special Publication, 800-10, December 1994.

Department of the Army, Technical Architecture, Version 4.5, November 12, 1996.

DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997.

JCSM, Secret and Below Interoperability, March 20, 1997.

Joint Staff briefing, Secret and Below Interoperability, Executive Status, February 24, 1998.

MCEB Draft Interim Planning Guidance, Information Assurance Roadmap.

MEDCOM, MEDCOM Internet Security Policy, January 16, 1996.

National Security Agency X3 Technical Report, Sidewinder V2.12 Analysis and Penetration Test Report, June 21, 1996.

National Security Agency X3 Technical Report, Trusted Information System's Gauntlet Version 3.0 Analysis and Penetration Test Report, May 26, 1996.

National Security Agency X3 Technical Report, V-One SmartWall Version 3.3.1 Analysis and Penetration Test Report, March 6, 1997.

Secret and Below Interoperability (SABI) Handbook, September 22, 1997 (FOUO).

A.2. Commercial Publications

Amoroso, Edward and Ronald Sharp, Intranet and Internet Firewall Strategies, Ziff-Davis Press, Emeryville, CA, 1996.

Atkins, Derek et al., Internet Security Professional Reference, New Riders Publishing, Indianapolis, IN, 1996.

Chapman, D. Brent and Elizabeth D. Zwicky, Building Internet Firewalls, O'Reilly and Associates, Inc. Sebastopol, CA, 1995.

Cheswick, William R. and Stephen M. Bellovin, Firewalls and Internet Security, Addison-Wesley Publishing Company, Reading MA, 1994.

Eagle NT 5.0., description, http//www.raptor.com/products/protuctsbriefs/neweagle.html.

Fuller, Scott and Kevin Pagan, Intranet Firewalls, Ventana Communications Group, Inc., Research Triangle Park, NC, 1997.

Goncalves, Marcus, Firewalls Complete, McGraw-Hill, New York, NY, 1998.

Goncalves, Marcus, Protecting Your Web Site with Firewalls, Prentice Hall PTR, Upper Saddle River, NJ, 1997.

National Computer Security Association, Firewall Buyer's Guide, 2nd Annual, 1998.

NSA MISSI Program's DMS Firewall Plus, http//www.wang.com/governmentservices/products/ssso/fw.html.

Siyan, Karanjit and Chris Hare, Internet Firewalls and Network Security, New Riders Publishing, Indianapolis, IN, 1995.

Appendix B, FIREWALL POLICY TEMPLATE

B.1 Background

This appendix contains a template that can be used in developing your firewall policy, an essential step before installing and configuring a firewall on your site. When considering firewall policies, it should be noted that there are two possible levels of firewall policy. The upper level policy is frequently called the firewall service access policy, and the lower level policy is called the firewall design policy. The service access policy focuses on presenting policy for what services will be allowed through the firewall. This appendix will not discuss the firewall design policy, which focuses on the specifics of how the service access policy will be implemented on a specific firewall, and instead is intended to provide guidance for a service access policy. The template includes minimum firewall policy statements and should be expanded or modified as necessary to meet local site or system requirements. The template does not address general policy statements that you may wish to add to your local policy. These general policy issues include items such as policy on the use of the Internet, policy on copyright violations, policy on use of Government systems and equipment, and other such general issues. These general policy issues are found in DOD, Army, or organizational directives or regulations and would not normally be included in a firewall policy document.

D.2 Assumption

It is assumed that before establishing the policy, an organization will have identified what needs to be protected, the protocols used, and the architecture of the system and firewall as discussed in the main body of this document.

B.3 Policy Format and Statements

The format chosen for the template, as shown in the sections that follow, is not as important as the information that should be included. An organization may choose to use their own format; as long as the general information is contained in the format, it will be an effective policy statement.

B.3.1 Purpose.

In this section there should be a clear-cut statement of the organization's policy for the

firewall. There are two fundamental policies that should be stated at the very beginning. These are:

Fundamental Policy No. 1: The firewall shall ensure that whatever is not expressly permitted is disallowed.

Fundamental Policy No. 2: The firewall must be installed so that all traffic between the protected network and the outside must go through the firewall.

The first fundamental policy has a weaker alternative which is, "whatever is not denied shall be permitted." This alternative should be rejected for Army firewalls. The second fundamental policy is absolutely essential for security. If there is even one modem behind the firewall, there is a backdoor to the protected network.

B.3.2 Responsibilities.

The policy document should have well-established, well-defined, and clearly documented responsibilities so that there is no misunderstanding about who is responsible for security measures relating to the firewall. The following are some of the more important responsibilities that should be assigned to particular individuals in the organization's firewall policy document. This in not intended to be an all-inclusive list of responsibilities, and an organization should consider expanding on the list in a policy document.

a. Chief Information Officer (CIO), Deputy Chief of Staff for Information Management (DCSIM), Director of Information Management (DOIM), Information Manager or equivalent will:

(1) Ensure that appropriate firewall security policies are established.

(2) Appoint a Designated Approving Authority (DAA) for the firewall and the organizational network it protects.

(3) Prepare budget and funding requests to support the firewall and other Command and Control Protect (C2P) requirements.

b. Designated Approving Authority (DAA). The DAA who has the responsibility for the firewall should be designated in the policy document, identified by position title. The DAA should be assigned the following responsibilities:

(1) Ensure that the firewall is accredited in accordance with the DOD Directive 5200.40 and AR 380-19.

(2) Coordinate accreditation of the firewall with other DAAs, as appropriate.

(3) Appoint an Information Systems Security Officer (ISSO) and an assistant ISSO with responsibility for the firewall.

(4) Ensure a firewall administrator and an assistant are appointed for the firewall.

(5) Review and approve the firewall security policy.

(6) Ensure the firewall security policies are enforced.

c. Information Systems Security Manager (ISSM). The ISSM has the following responsibilities for the firewall:

(1) Ensures the firewall policy is written that describes the intended functionality of the firewall and that the firewall as installed enforces that policy.

(2) Ensure the certification and accreditation paperwork is written on the firewall installation.

(3) Ensures that the firewall administrator (SA) receives training to operate the firewall.

d. Information Systems Security Officer (ISSO). The firewall ISSO has the following responsibilities for the firewall:

(1) Ensure that the firewall is operated and maintained according to the vendor's specifications and organizational requirements.

(2) Working with the firewall administrator, ensure that the firewall audit log is reviewed frequently.

(3) Report any security incidents involving the firewall as required by the organizational security regulations.

(4) Ensure the firewall security policy is implemented and carried out properly.

(5) Continuously evaluate the firewall security environment. Make recommendations to the DAA as appropriate.

d. Firewall Administrator. The firewall administrator has the following responsibilities:

(1) Understand and monitor the configuration of the firewall.

(2) Ensure that the firewall is continuously afforded effective physical security.

(3) Make frequent backups of data and files on the firewall and ensure that firewall software integrity is maintained.

(4) Respond to any alarms or alerts from the firewall software as quickly as possible.

(5) In coordination with the ISSO, ensure adequate security is maintained over the firewall.

(6) Install corrective patches to the firewall software as required.

(7) Review the audit logs on the firewall on a daily basis.

(8) Report any attacks or incidents on the firewall to the firewall ISSO.

(9) Evaluate each new release of the firewall software to determine if an upgrade is required and installing all security patches recommended by the vendor.

B.3.3 Policy Statements

This section should contain the firewall policy statements. The statements that follow should be considered for inclusion in the organization's firewall policy document:

a. Physical Security

(1) The firewall hardware shall be located in a controlled environment with unescorted access limited to the ISSO, the firewall administrator, and their alternates.

(2) Anyone entering the firewall enclosure without unescorted access privileges shall sign a visitor's log before entering and upon leaving the firewall enclosure.

(3) The firewall enclosure shall be equipped with heat, air conditioning, and smoke alarms to ensure a proper operating environment for electronic equipment.

(4) The firewall shall be protected against unauthorized hardware or software modifications.

b. Firewall Administrative Security

(1) The firewall administrator and the alternate shall be trained in administration, operation, and maintenance of the firewall.

(2) The firewall administrator, ISSO, and their alternates shall be designated as ADP-I positions and the individuals filling those positions shall have the appropriate background investigations for those positions as specified in AR 380-67.

(3) The firewall shall be accredited in accordance with the DITSCAP after installation. Reaccreditation shall be in accordance with paragraph 3-6 of AR 380-19.

(4) Systems that are to be protected by the firewall shall be explicitly identified.

(5) Deliberate violations of this firewall policy document shall be subject to appropriate disciplinary action based on the severity of the violation.

c. Firewall Policies

(1) The firewall must be located and configured so that it can monitor and control all communications between the protected network and the systems on the outside of the firewall.

(2) There shall be no modems or dial-in or dial-out connections on the protected network that do not go through the firewall. As an exception, a dial out only modem may be permitted for notifying security personnel of a security event by pager. The modem must be configured to allow only one single phone number for this purpose.

(3) The firewall must be configured so that it cannot be bypassed or circumvented.

(4) The firewall must be configured to withstand deliberate denial-of-service attacks such as SYN flooding or "ping of death" attacks.

(5) Direct login to the firewall shall be from the firewall keyboard only; no indirect logins shall be permitted. Direct login privilege shall be restricted to the firewall administrator, the ISSO, and their alternates. Per DA policy, ANSOC will be provided passwords and also monitor firewalls.

(6) Any modification of the firewall software must be done by the firewall administrator or alternate administrator.

(7) The firewall shall require strong authentication before permitting a process to pass through to the protected network.

(8) The firewall shall be configured to be capable of establishing a virtual private network (VPN) with another Army site.

(9) The firewall shall be configured to be capable of passing encrypted information.

(10) The firewall shall be configured to be capable of detecting, prohibiting, and reporting a hacker's attempt to do port scanning.

(11) The firewall shall be configured to be capable of detecting, prohibiting, and reporting use of the SATAN tool.

(12) The firewall may not have any compilers, editors, communications software, user applications, or any other files on the firewall other than those directly related to the functioning of the firewall. An intrusion detection system is permitted as an exception.

(13) The firewall shall report, or log, all violations of this policy.

(14) The threshold for reporting or logging incidents or policy violations shall be configured as (specify) incidents.

(15) The audit trail or logs shall be maintained in files accessible only by the firewall administrator, the ISSO, or their alternates.

(16) The firewall audit trail, or event logs, shall be reviewed by the firewall administrator, or the ISSO, or their alternates on a (specify – but preferably daily) basis.

(17) The firewall audit trail, or event logs, shall be maintained on file (specify type of file, i.e., floppy disk) for a period of (specify) months. (Key here is to make the retention period long enough to be able to analyze any incidents that occur in the recent past.)

(18) Alarm and alert functions on the firewall and any other perimeter access control devices shall be enabled.

(19) The firewall administrator shall be notified at anytime of any security alarm by the fastest means possible so that an immediate response may be made to the alarm.

(20) System integrity checks of the firewall shall be performed on a routine basis.

(21) System users shall receive security awareness training so that they do not compromise the firewall's security processes.

(22) Application level firewalls shall be configured so that outbound network traffic appears as if the traffic had originated from the firewall, i.e., internal addresses are hidden from the outside networks.

(23) All inbound Internet services must be processed by proxy software supported by the firewall. If a new service is requested, that service shall not be made available until a proxy is available on the firewall.

(24) The firewall's system integrity database shall be

updated each time the firewall's configuration is modified. System integrity files shall be stored on read-only media or on off-line storage media.

(25) The firewall should fail to a configuration that denies all services, and should require the firewall administrator to re-enable services after a failure.

(26) Source routing shall be disabled on the firewall.

(27) The firewall shall be configured to reject all traffic on its external interfaces that appears to be coming from internal network addresses.
(28) The firewall shall notify the firewall administrator in near real-time of any item that may need immediate attention, so that immediate action may be taken.

(29) The firewall shall have an uninteruptable power supply (UPS). The UPS should have sufficient capacity to facilitate proper shutdown of a firewall.

(30) The firewall shall have backups of all relevant data and files and backups shall be stored in a different secure location. Backups can be used to restore operations. If backups are near firewall, they may succumb to the same fate as the firewall.

(31) The firewall shall have a Continuity of Operations Plan (COOP).

d. Protocol and Port Policies

There are two categories of protocols that are considered by the firewall. First are the protocols and their corresponding ports that are authorized for passing through the firewall. This category will have some protocols that are one-way, either outbound or inbound. The other category are the protocols and ports that are prohibited from transiting the firewall, primarily because of security issues. These protocols and their policy statements are listed below: (Note: This list should be modified to meet your local requirements. However, the prohibited protocols should not normally be allowed without some special justification, and the DAA should be made aware of the dangers if a prohibited protocol is allowed on a firewall.)

(1) Allowable protocols. The following protocols and ports may be allowed to pass through the firewall, or to be handled by proxies. This list of protocols includes all the protocols listed in Tables 1 and 2 of the main body of this guidance. The list of allowable protocols should be considered as "candidates" for passing through the firewall as each site should individually determine what they will allow through. (It is important to note that even though the list below states that it shall be permitted, if the protocol is NOT used on a particular site, it should still be blocked.)

(a) Common Management Information Protocol (CMIP), ports 163 and 164. CMIP shall be allowed through the firewall. The authentication, access control, and security log features shall be enabled.

(b) Domain Name System (DNS), port 53. DNS shall be

allowed outbound to access name servers. DNS shall not be allowed inbound as the firewall should conceal the inside addresses.

(c) Echo (ping) Command, port 7. The firewall shall be configured to permit outbound "Echo request" (ping) packages and inbound "Echo response" to pass through the firewall, but disallow incoming "Echo request" packets.

(d) Endpoint Map (epmap), port 135. If RPC is enabled (see below), epmap shall be allowed through the firewall.

(e) File Transfer Protocol (FTP), ports 20 and 21. FTP should be permitted to pass through the firewall outbound. Inbound FTP traffic should only be allowed through the firewall from specific IP addresses.

(f) Finger command. The finger command shall be permitted to pass through the firewall outbound, but all incoming finger requests shall be blocked.

(g) Gopher, ports 70 and >1023. Gopher shall only be used if proxied at the firewall and shall be configured only for outbound use.

(h) Hypertext Transport Protocol (HTTP), ports 1023 and 80. The HTTP protocol shall only be used if a proxy exists on the firewall.

(i) Internet Control Message Protocol (ICMP). The firewall shall be configured to drop packets without returning an ICMP error message.

(j) Internet Protocol (IP). The firewall shall be configured to drop all packets arriving on the unprotected side with a source address of a machine on the protected side.

(k) Internet Packet Exchange (IPX), port 213. If used on a site, the IPX protocol shall be permitted through the firewall.

(l) International Standards Organization-Transport Layer Service Access Protocol (ISO-TSAP), port 102. The ISO-TSAP protocol shall be allowed through the firewall. For outbound packets, the packet's source address shall be changed to the firewall's address.

(m) Multipurpose Internet Mail Extension (MIME). MIME shall be permitted through the firewall.

(n) Post Office Protocol 3, port 110. POP3 traffic shall be permitted to pass through the firewall, but only to the SMTP server.

(o) Remote Procedure Call (RPC), port 530. RPCs shall only be permitted outbound. The firewall shall prohibit all inbound RPCs.

(p) Secure Electronic Transaction (SET), port 257. SET shall be permitted to pass through the firewall.

(q) Secure Hypertext Transfer Protocol (S-HTTP), port 443. S-HTTP shall be permitted through the firewall.

(r) Secure Multipurpose Internet Mail Extension (S-MIME). S-MIME shall be permitted through the firewall.

(s) Secure Socket Layer (SSL), port 443. SSL shall be permitted through the firewall.

(t) Simple Mail Transfer Protocol (SMTP), port 25. SMTP shall be permitted through the firewall, but only to the mail server on the protected side.

(u) Telecommunications Network (TELNET), port 23. TELNET shall be permitted to pass outbound through the firewall, but shall be prohibited from coming in through the firewall to the protected side.

(v) Terminal Access Controller Access Control System (TACACS), port 49. TACACS shall be permitted through the firewall.

(w) Transmission Control Protocol (TCP). TCP shall be permitted through the firewall. The firewall shall be configured to prevent "SYN flood" attacks.

(x) User Datagram Protocol (UDP). UDP shall be permitted through the firewall, but the firewall shall block all UDP packets inbound with a host address of a machine on the protected side.

(y) Virtual Private Network (VPN). The firewall shall establish VPNs whenever possible.

(z) Whois Command, port 43. The firewall shall permit outbound whois traffic, but shall block all inbound use of the whois command.

(2) Prohibited Protocols. In accordance with Fundamental Policy No. 1 listed in paragraph 3.(1)a of this appendix, there is no need to list prohibited protocols since they are blocked if they are not expressly permitted. However, if desired, the following policy statements could be included.

(a) Archie, port 1525 and >1023. Port 1525 shall be blocked by the firewall.

(b) Exterior Gateway Protocol (EGP). EGP requests shall not be permitted through the firewall.

(c) Internet Relay Chat (IRC), port 194. Port 194 shall be blocked by the firewall.

(d) Network Basic Input/Output Services (NetBIOS), ports 137 – 139. Ports 137, 138, and 139 shall be blocked by the firewall. Blocking these ports does not limit the use of NetBIOS on the protected side.

(e) Network File System (NFS), port 2049. Port 2049 shall be blocked by the firewall.
(f) Network Information Service (NIS). NIS traffic shall not be permitted through the firewall.

(g) Network News Transfer Protocol (NNTP), port 119. Port 119 shall be blocked by the firewall.

(h) Network Time Protocol (NTP), port 123. Port 123 shall be blocked by the firewall.

(i) Open Shortest Path First (OSPF). OSPF traffic shall not be permitted through the firewall.

(j) Open Windows, port 2000. Port 2000 shall be blocked by the firewall.

(k) Remote Execution (rexec), port 512. Port 512 shall be blocked by the firewall.

(l) Remote Hosts (rhost). The system shall not allow the use of .rhost files.

(m) Remote Login (rlogin), port 513. Port 513 shall be blocked by the firewall.

(n) Restricted Shell (rsh), port 514. Port 514 shall be blocked by the firewall.

(o) Remote Access Protocol (RAP), port 38. Port 38 shall be blocked by the firewall.

(p) Routing Information Protocol (RIP), port 520. Port 520 shall be blocked by the firewall.

(q) Simple Network Management Protocol (SNMP), ports 161 and 162. Ports 161 and 162 shall be blocked by the firewall.

(r) Trivial File Transfer Protocol (TFTP), port 69. Port 69 shall be blocked by the firewall.

(s) UNIX-to-UNIX Copy (UUCP), port 540. Port 540 shall be blocked by the firewall.

(t) Wide-Area Information Service (WAIS), ports 210 and >1023. Port 210 shall be blocked by the firewall.

(u) X-Windows (X11), port 6000-6063. Port 6000-6063 shall be blocked by the firewall.

Appendix C, GUARD POLICY TEMPLATE

C.1 Background

This appendix contains a template that can be used in developing a guard policy document. Of necessity it must be more incomplete than the firewall policy template in Appendix D, since so much of the guard's functioning is dependent on how the guard is used, and not related to protocols. The use of guards relates to DoD's SABI program, but unfortunately the SABI Handbook, dated 22 September 1997, provides no assistance in determining guard policies. However, it does point out one key element in establishing a guard policy, and that is that the initial step must be to determine the system and guard requirements. This step involves an analysis of needs and usage requirements, and should include developing a concept of operations for the guard.

C.2 Assumptions

It is assumed that before establishing the policy, an organization will have identified what needs to be protected, the protocols used, and the architecture of the system and guard as discussed in the main body of this document.

C.3 Policy Format and Statements

The format in the sections that follow attempts to present a thought process to be followed, rather than presenting precise format statements as was the case in the firewall policy template.

C.3.1 Purpose

The organization's policy for the guard should be stated in this section. The guard's basic

function is to protect the confidentiality of higher classified information when two systems of different classification levels are interconnected. The purpose should specifically state whether bi-directional flow of information is to be processed by the guard, or only from high to low. As with the firewall policy, there are two fundamental policies that should be stated at the very beginning. These are:

Fundamental Guard Policy No. 1: The guard shall ensure that whatever is not expressly permitted is disallowed.

Fundamental Guard Policy No. 2: The guard must be the only connection between two networks of different classification levels, and any information flow between the networks shall only be through the guard.

In many guard implementations there is a companion policy to Fundamental Policy No. 1 which states that:

Companion Policy: Any traffic that the guard rejects shall be placed in a buffer for manual review by the guard administrator or security officer.

The companion policy assumes that the man-in-the-middle concept is being used for the guard.

C.3.2 Responsibilities

The guard security policy document, like the firewall policy, should have well-established, well-defined, and clearly documented responsibilities so that there is no misunderstanding about who is responsible for security measures relating to the guard implementation. The following are some of the more important responsibilities that should be assigned to particular individuals in the guard security policy document. This is not intended to be an all-inclusive list of responsibilities, and an organization should consider expanding the list in a guard security policy document.

a. Chief Information Officer (CIO), Deputy Chief of Staff for Information Management (DCSIM), Director of Information Management (DOIM), Information Manager, or equivalent will:.

(1) Ensure that appropriate guard security policies are established.

(2) Appoint a Designated Approving Authority (DAA) for the guard and the organizational networks it connects. There may be a DAA appointed for each network, in which case both DAAs will coordinate in the accreditation of the guard.

(3) Prepare budget and funding requests to support the guard and other Command and Control Protect (C2P) requirements.

b. Designated Approving Authority (DAA). The DAA, who has the primary responsibility for the guard and the network it is attached to, should be designated in the policy document, identified by billet title. The policy should also identify the DAA for the other network that the guard is attached to, identified by billet

title. This second DAA is a supporting DAA. The primary DAA should be assigned the following responsibilities:

(1) Ensure that the guard and the network it is attached to are accredited in accordance with DOD Directive 5200.40 and AR 380-19.

(2) Coordinate accreditation of the guard with the DAA of the other network as appropriate.

(3) Appoint an Information Systems Security Officer (ISSO) and an assistant ISSO with responsibility for the guard. The ISSO in this case may be one of the network ISSOs, but it is important that someone be assigned responsibility for overseeing the guard's functioning.

(4) Ensure a guard administrator and an assistant are appointed. This administrator may be one of the network systems administrators, but the key issue is that someone is assigned responsibility for the technical configuration of the guard.

(5) Review and approve the guard security policy.

(6) Ensure the guard security policies are enforced.

c. Information Systems Security Manager (ISSM). The ISSM has the following responsibilities for the guard:

(1) Ensures the guard policy is written that describes the intended functionality of the guard and that the guard as installed enforces that policy.

(2) Ensure the certification and accreditation paperwork is written on the guard installation.

(3) Ensures that the firewall administrator (SA) receives training to operate the guard.

d. Information Systems Security Officer (ISSO). The ISSO assigned responsibilities for the guard has the following responsibilities for the guard's functions:

(1) Ensure that the guard is operated and maintained according to the vendor’s specifications and organizational requirements.

(2) Working with the guard administrator, ensure that the guard audit log is reviewed frequently.

(3) Report any security incidents involving the guard as required by the organizational security regulations.

(4) Ensure the guard security policy is implemented and carried out properly.

(5) Continuously evaluate the guard security environment. Make recommendations to the DAA as appropriate.

d. Guard Administrator. The guard administrator has the following responsibilities:

(1) Understand and monitor the configuration of the guard.

(2) Ensure that the guard is continuously afforded effective physical security.

(3) Make frequent backups of data and files on the guard and

ensure that guard software integrity is maintained.

(4) Respond to any alarms or alerts from the guard software as quickly as possible.

(5) In coordination with the ISSO, ensure adequate security is maintained over the guard.

(6) Install corrective patches to the guard software as required.

(7) Review the audit logs on the guard on a daily basis.

(8) Report any attacks or incidents on the guard to the guard ISSO.

(9) Evaluate each new release of the guard software to determine if an upgrade is required and install all security patches recommended by the vendor.

e. Man-in-the-Middle (MIM). (This section should only be included if the guard has a MIM capability. A MIM is the human responsible for reviewing all files rejected by the guard and is a generic firewall term, not related to the gender of the individual performing that function. Many modern guards have eliminated the use of a MIM.) The MIM has the following responsibilities:

(1) Reviewing all files rejected by the firewall to determine if they can be transmitted to the lower classification level.

(2) Downgrading all rejected files after a review indicates that action is appropriate. The files should then be forwarded to the guard for action.

(3) Securely destroying all files that the review indicates cannot be downgraded.

(4) Monitoring the guard's functioning by periodically reviewing messages automatically forwarded by the guard.

C.3.3 Policy Statements

This section should contain the guard policy statements. The statements that follow should be considered for inclusion in the organization's guard policy document:

a. Physical Security

(1) The guard hardware shall be located in a controlled environment with unescorted access limited to the ISSO, the guard administrator, and their alternates.

(2) Anyone entering the guard enclosure, defined as the room in which the guard is placed, without unescorted access privileges shall sign a visitor's log before entering and upon leaving the guard enclosure.

(3) The guard enclosure shall be equipped with heat, air conditioning, and smoke alarms to assure a proper operating environment for electronic equipment.

(4) The guard shall be protected against unauthorized hardware or software modifications.

b. Guard Administrative Security

(1) The guard administrator and the alternate shall be trained in administration, operation, and maintenance of the guard.

(2) The guard administrator, ISSO, and their alternates shall be designated as ADP-I positions and the individuals filling those positions shall have the appropriate background investigations for those positions as specified in AR 380-67.

(3) The guard shall be accredited in accordance with the DITSCAP after installation. In this regard, accreditation of the guard will be included in the accreditation of one of the networks it connects to. A separate accreditation of the guard alone shall not be required. Reaccreditation shall be in accordance with paragraph 3-6 of AR 380-19.

(4) Networks that are connected by the guard shall be explicitly identified.

(5) Deliberate violations of this guard policy document shall be subject to appropriate disciplinary action based on the severity of the violation.

c. Guard Policies

(1) The guard must be located and configured so that it can monitor and control all message traffic between the two networks.

(2) There shall be no other connections between the two networks other than through the guard.

(3) Direct login to the guard shall be from the guard keyboard only; no indirect logins shall be permitted. Direct login privilege shall be restricted to the guard administrator, the ISSO, and their alternates.

(4) Direct login to the MIM workstation shall be from the MIM workstation keyboard only; no indirect logins shall be permitted. Direct login privilege shall be restricted to the MIM, the guard administrator, the ISSO, and their alternates. (Include only if applicable.)
(5) Any modification of the guard software must be done by the guard administrator or alternate administrator.

(6) The guard shall not pass any encrypted files.

(7) The guard shall be configured to be capable of detecting, prohibiting, and reporting a hacker's attempt to do port scanning.

(8) The guard shall be configured to be capable of detecting, prohibiting, and reporting use of the SATAN tool.

(9) The guard may not have any compilers, editors, communications software, user applications, or any other files on the guard other than those directly related to the functioning of the guard.

(10) The guard shall report, or log, all violations of this policy.

(11) The threshold for reporting or logging incidents or policy violations shall be configured as (specify) incidents.

(12) The audit trail or logs shall be maintained on files accessible only by the guard administrator, the ISSO, or their alternates.

(13) The guard audit trail, or event logs, shall be reviewed by the guard administrator, or the

ISSO, or their alternates on a (specify – but preferably daily) basis.

(14) The guard audit trail, or event logs, shall be maintained on file (specify type of file, i.e., floppy disk) for a period of (specify) months. (Key here is to make the retention period long enough to be able to analyze any incidents that have occurred in the recent past.)

(15) Alarm and alert functions on the guard shall be enabled.

(16) The guard administrator shall be notified at anytime of any security alarm by the fastest means possible so that an immediate response may be made to the alarm.

(17) System integrity checks of the guard shall be performed on a routine basis.

(18) The default condition shall be no transfers from the higher classified network to the lower network.

(19) The guard shall check all attachments to files before transferring them.
(20) The guard will not perform virus checks. Before submitting a file to the guard a user should ensure that the file does not contain a virus.
d. Functional Policies

The guard has three functional checks that it makes. This section of the policy should specify what action the guard should take for each type of check. The following contains questions or actions that should be considered in writing the policy for a specific guard implementation. The key is to include all actions that the guard should take and specify them in clear, concise terms.

(1) Format Checking. Format checking is specific to a particular type of document or format and requires precise determination of the format that should be checked. Some of the items that you should consider putting into the file include:

a. Checking for the presence of the classification in the header and/or footer of the page.

b. Checking for the presence of security labels at the beginning of a paragraph such as (U) or (S).

c. Checking for the classification in a particular field or location in a file or message.

d. Checking for attachments to messages or files.

e. Specifying the action to be taken if violations are found, for example, is the guard expected to make the appropriate substitutions in the field or the document to correct the violation?

f. What procedures are to be followed for changing the formats being checked?

g. What actions does the guard take if a format check fails?

h. What messages does the guard send regarding format checking actions?

i. What logging does the guard perform regarding format checking?

(2) Dirty Word Checking. A “dirty word” in this sense is a word that either is classified, i.e., a code word, or a word indicating a higher classification than the lower system is cleared to process. Some of the items that should be considered for inclusion in this section are:

a. Specifying if the checking is full text or only specific fields.

b. Specifying the dirty word in all possible combinations. This is a difficult task as illustrated by the classification, “top secret.” You would want to look for: TOP SECRET, Top Secret, TS, (TS), top secret, Top secret, top SECRET, and all other variations of the words. If your system processes foreign documents, the dirty word may be the classification label in the foreign language, which will further complicate your problem.

c. Specifying all highly classified dirty words, for example, “Manhattan Project” or “Operation Overlord.” In this context, it is important to note that a date or a particular number could also have a dirty word connotation. Identifying this type of dirty word will be more difficult than merely handling the classification labels in their various forms.

c. What actions does the guard take if a dirty word check fails?

d. What messages does the guard send regarding dirty word checking actions?

e. What logging does the guard perform regarding dirty word checking?

(3) Context Checking. Having a guard do context checking is even harder to put into words that the guard can enforce. As with the other checks above, you will have to identify the context in which a term has a higher classification than the term by itself. For example, once the code word "Operation Overlord" was revealed as being the name for the invasion of Europe, using those words in connection with France would again be highly classified. Dates, numbers, or organizations used in relation with planned operations is another example. The term, 29th Infantry Division, by itself means nothing, but when used in connection with 6 June 1944 would have been highly classified. In relation to context checking, the policy would include:

a. Specifying the precise context that the guard should search for.

b. Specifying if the context checking is full text or only specific fields.

c. What actions does the guard take if a context check fails?

d. What messages does the guard send regarding context checking actions?

e. What logging does the guard perform regarding context checking?

Appendix D, SAMPLE MOU/MOA

MEMORANDUM OF AGREEMENT (UNDERSTANDING)

1. This agreement is between < DAA FOR POST ARMY NETWORK > and < DAA FOR OTHER NETWORK (CORPS OF ENGINEERS, MEDICAL, DREN)>

2. The purpose of this agreement is to define the terms and conditions under which the < OTHER NETWORK (CORPS OF ENGINEERS, MEDICAL, DREN)> will be connected to the <location> post network.

3. The documents in Table 6 describe the <OTHER NETWORK (CORPS OF ENGINEERS, MEDICAL, DREN)>.

Table 6. Documents Needed for Post Connection
1 A Letter of Accreditation or Interim Authority to Operate (from the SSAA see paragraph 2.5.2)
2 An installation system connectivity diagram for the installation
3 A Consent to Monitor statement
4 A statement of significant or residual risk
5 Non-DOD connections (e.g., contractor, foreign, etc.)
6 A Statement of minimal security requirements as stated in the accreditation plan
7 A Statement of specific security features and implementations, such as firewalls, guards, and secure network servers, as stated in the security concept of operations
8 Copies of any memorandums of agreement/understanding (MOA/MOU) with any other interconnected systems or networks
9 The mode of operation
10 The maximum level of sensitivity of information processed

4. Both parties agree to immediately inform each other of any security incidents or change to risks on either network.

5. The following points of contact will be used:

a. For command related items:

b. For security related items:

c. For daily operations:

Signature and signature blocks of respective DAAs

Appendix E

SSAA OUTLINE AND DETAILED DESCRIPTION

1.1. SSAA OUTLINE

1.1.1. Document. The SSAA is a living document that represents the formal agreement between the DAA, CA, PM and user representative. The SSAA is developed in Phase 1 and updated in each phase as the system development progresses and new information becomes available. At a minimum, the SSAA should contain the information in the following sample outline:

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1. System name and identification

1.2. System description

1.3. Functional description

1.3.1. System capabilities

1.3.2. System criticality

1.3.3. Classification and sensitivity of data processed

1.3.4. System user description and clearance levels

1.3.5. Life-Cycle of the system

1.4. System CONOPS summary

2. ENVIRONMENT DESCRIPTION

2.1. Operating environment

2.2. Software development and maintenance environment

2.3. Threat description

3. SYSTEM ARCHITECTURAL DESCRIPTION

3.1. Hardware

3.2. Software

3.3. Firmware

3.4. System interfaces and external connections

3.5. Data flow (including data flow diagrams)

3.6. TAFIM DGSA (reference (av)) security view

3.7. Accreditation boundary

4. ITSEC SYSTEM CLASS

4.1. Interfacing mode

4.2. Processing mode

4.3. Attribution mode

4.4. Mission-reliance factor

4.5. Accessibility factor

4.6. Accuracy factor

4.7. Information categories

4.8. System class level

4.9. Certification analysis level

5. SYSTEM SECURITY REQUIREMENTS

5.1. National/DoD security requirements

5.2. Governing security requisites

5.3. Data security requirements

5.4. Security CONOPS

5.5. Network connection rules

5.5.1. To connect to this system

5.5.2. To connect to the other systems defined in the CONOPS

5.6. Configuration and change management requirements

5.7. Reaccreditation requirements

6. ORGANIZATIONS AND RESOURCES

6.1. Identification of organizations

6.1.1. DAA

6.1.2. Certification authority

6.1.3. Identification of the user representative

6.1.4. Identification of the organization responsible for the system

6.1.5. Identification of the program manager or system manager

6.2. Resources

6.2.1. Staffing requirements

6.2.2. Funding requirements

6.3. Training for certification team

6.4. Roles and responsibilities

6.5. Other supporting organizations or working groups

7. DITSCAP PLAN

7.1. Tailoring factors

7.1.1. Programmatic considerations

7.1.2. Security environment

7.1.3. IT system characteristics

7.1.4. Reuse of previously approved solutions

7.1.5. Tailoring summary

7.2. Tasks and milestones

7.3. Schedule summary

7.4. Level of effort

7.5. Roles and responsibilities

1.1.2. Appendices. Appendices should include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation relevant to the systems' C&A.

APPENDIX A Acronym List

APPENDIX B Definitions

APPENDIX C References

APPENDIX D Security Requirements and/or Requirements Traceability Matrix

APPENDIX E Security Test and Evaluation Plan and Procedures

APPENDIX F Certification Results

APPENDIX G Risk Assessment Results

APPENDIX H CA's Recommendation

APPENDIX I System Rules of Behavior

APPENDIX J Contingency Plan(s)

APPENDIX K Security Awareness and Training Plan

APPENDIX L Personnel Controls and Technical Security Controls

APPENDIX M Incident Response Plan

APPENDIX N Memorandums of Agreement - System Interconnect Agreements

APPENDIX O Applicable System Development Artifacts or System Documentation

APPENDIX P Accreditation Documentation and Accreditation Statement

1.2. SSAA DETAILED DESCRIPTION

Each section of the SSAA is briefly described below.

1.2.1. Mission Description and System Identification. This section must describe the system and the mission that the system supports. This includes a statement on how the system's mission supports the organization's mission, the name of the organization, the system's name, the longevity and the placement of the system within its life-cycle, a discussion of the information categories to be processed to support the mission, a high level information flow specification, a functional description, a statement on personnel clearances, and a stipulation of the system criticality. The mission description is a concise, high level system specification and needs statement. It describes whom the system will serve, how it will work, what information it will process, how important it is, and why it is being

developed. The mission description must focus on the ITSEC relevant features of the system. This section does not contain implementation specifics. The mission description should come from the mission need document (e.g., Mission Need Statement, Mission Impact Statement, Operational Requirements Document, the purpose statement of the using organization). See Task 1-1 in Chapter 3 for additional details on how to prepare this section.

1.2.1.1. System Name and Identification. This section should identify the system that is being developed or entering the ITSEC C&A process. This section provides the name and organization of the element developing the mission need and the organizations containing the ultimate user. It identifies the general user who helps to define operational scenarios that may be encountered, especially for tactical systems.

1.2.1.2. System Description. The system description should provide a complete high-level description of the system architecture. Diagrams or drawings should be included to amplify the description. All components of the system should be described. If the information is insufficient or the understanding of the system is insufficient for the system description to be written, the system is not ready to begin the C&A process. The system description should include all critical elements required for the mission need.

1.2.1.3. Functional Description. This section provides a functional description of the system and the purpose or mission for which it will be used. Include functional diagrams of the system. Describe functions performed jointly with other systems and identify the other systems. Include high level functional diagrams. Provide the intended flows of data into the system, data manipulation, and product output. The mission need should clearly state the purpose for which the system is needed and the capabilities desired. For example, a system is required for a local area network (LAN) within an office environment to permit the access of all LAN stations to LAN server resources. In addition, connectivity is required to a wide area network (WAN) for interactive sessions with all other resources having access to the WAN.

1.2.1.3.1. System Capabilities. The system functional description and system capabilities information provides a summary of the system mission and function statements. The system capability description should clearly delineate what function or capability is expected to be present in the fully accredited system.

1.2.1.3.2. System Criticality. This section examines the consequences of a loss of the system. It assesses the effect on DoD operations, the various Military Departments, or other government agencies if they were denied the reliable use of this system. From this analysis, a determination of the system's criticality is made.

1.2.1.3.3. Classification and Sensitivity of Data Processed. This section should state the general classification of information intended (unclassified, confidential, secret, top secret) along with any special compartment or subcompartments. The mission need statement should be examined to determine the classification of information to be processed

(unclassified, confidential, secret, top secret) along with any special compartment. The information category will also be used to determine the overall system class. This requires the identification of the type of information processed (Privacy Act, financial, critical operational, proprietary, and administrative).

1.2.1.3.4. System User Description and Clearance Levels. The ultimate security architecture, level of security assurance, and security design requirements depends on the security clearances of the users, the users' access rights to the specific categories of information processed, and the actual information the system is required to process. It is essential that the mission need clearly state the user population's security clearances and access rights to other restricted information. For example, a system may be required to have contractor personnel as authorized users; however, under classification of data processed, the mission need states that proprietary information from commercial organizations other than the users would be processed. This situation creates a security problem in that sufficient controls must be designed into the system to preclude having the contract users gain intentional or unintentional access to the proprietary data.

1.2.1.3.5. Life-Cycle of the System. This section describes the life-cycle and where the system is in relationship to its life-cycle. For example, if the mission need states that a sensor support system is needed urgently to provide tactical support to ongoing operations, an accelerated development and acquisition process is most likely to be used. The C&A process must be prepared to keep pace with this effort, and that requires resource allocation on the part of the CA and DAA.

1.2.1.4. System CONOPS Summary. This information supplements the system description and function statements. What is needed in this section is a high level description of the concept for the system to satisfy the mission need. Provide a description of those functions that are jointly performed with other systems, and identify the other systems.

1.2.2. Environment Description. The environment description documents the intended operational environment, software development and maintenance environment, the threat environment, external electronic connections, and the political environment (if applicable). This will include the connection layer information. If more than one location is used, provide details for each as a separately numbered heading. See Task 1-3 in Chapter 3 for additional details on how to prepare this section.

1.2.2.1. Operating Environment. Identify and describe the physical environment in which the IT system will operate including floor plans, equipment placement, electrical and plumbing outlets, and telephone outlets. Describe the access control procedures provided by the environment and any other standard operating procedures that support a secure environment. Include existing security features mandated by the operational situation in this section. Provide a description of existing environmental security features that will mitigate the implementation of specific security requirements in that environment rather than in the system architecture and design.

1.2.2.2. Software Development and Maintenance Environment. Identify and describe the software development and maintenance environment - open or closed. See Task 1-3 in Chapter 3 for additional details.

1.2.2.3. Threat Description. Identify and describe the vulnerability-induced threats, environmentally based threats, and the impact these threats have on mission need. Definition of the potential threats must consider the intentional and unintentional events that can affect the integrity, confidentiality, and availability of the system.

1.2.3. System Architectural Description. The architecture description provides the framework for the information system architecture and includes a physical description of the hardware, software, firmware, and interfaces. Against this framework, the architecture description stipulates the security architecture. Existing or planned system features that facilitate expansion or external connection should be mentioned in this section. During the concept development phase, the architecture may not be fully developed. A broad description of these areas may be provided. However, once the information system has entered the design phase, the architecture description must be updated and details provided. Areas may exist that do not apply to the information system (e.g., firmware). In that case, it is appropriate to enter the term non-applicable. Adequate detail should be included to compare the system's architecture with the DGSA. Task 1-4 in Chapter 3 provides additional details on this section of the SSAA.

1.2.3.1. Hardware. Identify and describe the hardware used and whether it is a standard commercial product, unique, or on the EPL. Include an equipment list as an attachment. Describe the target hardware and its function. Hardware is the physical equipment as opposed to programs, procedures, rules, and associated documentation. If this development effort involves an existing hardware change, identify the specific hardware components being changed.

1.2.3.2. Software. Identify and describe the operating system(s), database management system(s), and applications. Identify and describe the features of any security packages used on the information system. Identify any software packages that are COTS, GOTS, and on the EPL. Describe the target software and its intended use. Software includes the entire set of application programs, software procedures, software routines, and operating system software associated with the system in question. This includes manufacturer supplied software, other commercial off-the-shelf software, and all program generated applications software.

1.2.3.3. Firmware. Identify and describe the firmware used and whether it is a standard commercial product, unique, or on the EPL. Describe the software that is stored permanently in a hardware device that allows reading and executing the software, but not writing or modifying it. For example, items such as programmable read-only memory (PROM) and enhanced PROM (EPROM) devices are considered firmware.

1.2.3.4. System interfaces and external connections. Provide a statement of the significant features of the communications layout. Include a

high level diagram of the communications links and encryption techniques connecting the components of the information system, associated data communications, and networks.

1.2.3.5. Data flow (including data flow diagrams). Describe the system's external interfaces. The description must include a statement of the purpose of each external interface and the relationship between the interface and the system. The types of data and the general methods for data transmission should be stated if specifically required. If specific transmission media are not necessary for the mission need, the mission need should state the basic transmission capability desired. From this the security engineer, working with the PM, can make an initial assumption on a suitable method for processing the data flow requirements.

1.2.3.6. TAFIM DGSA, Security View. Provide a comparison of the significant features of the information system's architecture to the DGSA. Include a diagram of the relationship of the system architecture to the DGSA.

1.2.3.7. Accreditation Boundary. Describe the boundary of the system under consideration. The description must include diagrams or text to clearly delineate which components are to be evaluated as part of the C&A task, and which are not included. All components included must be described in the systems description. Elements outside the accreditation boundary must be included in the description of the external interfaces.

1.2.4. ITSEC System Class. This section specifies the system based on an assessment of the information provided. The containment, system use level and information categories determine the IT system class. The IT system class is used to specify the certification level. Appendix 2 provides a description of the process to determine the system class and certification level. These sections of he SSAA should document the results of determining the system class.

1.2.5. System Security Requirements. The system security requirements are derived from the security policy. Examples of requirements are Identification and Authentication (I&A), contingency planning, access controls, etc. The security analysis levels stipulate the high-level security requirements. Once the system class has been determined, use the repository to assist in identifying the system security requirements. Include those required by directives, those due to connection with other networks and systems, those required by data originators, and any additional requirements specified by the DAA. Requirements of all ITSEC disciplines (Computer Security (COMPUSEC), COMSEC, TEMPEST, physical security, and personnel security) must be included. A common approach to prepare this section is to construct a RTM. Chapter 3, Table C3-8 provides an example of an RTM matrix. (The review column identifies the review process for each requirement, where I - Interview, D - Document review, T - Test, and O - Observation.) Another example may be found on the IASE.

1.2.5.1. National/DoD security requirements. In most cases, this will include information derived from Public Laws, national Act's, national level directives, OMB Circulars A-123 and OMB A-130 (references (m) and (d)),

and DoD directives. There are usually a number of service or agency directives that also dictate security requirements for the system. In all cases, all the directives that will impact the ultimate user should be included in this section. Within the U. S. Government, many systems are required to meet the requirements of the Trusted Computer Security Evaluation Criteria, TCSEC, and (reference (n)). In these cases, the certification team should obtain the requirements for that level, e.g., level C2.

1.2.5.2. Governing Security Requisites and Data Security Requirements. In addition to the requirements defined in instructions and directives, there may be security requirements stipulated by local agencies and the DAA. The DAA and user representative should be able to supply this information. It should be referenced in this section and added to the RTM. The type of data to be processed may result in additional restrictions as determined by the data owner or organizations that have access to the system or share data with the system. If this is the case, that information should also be referenced in this section and added to the RTM.

1.2.5.3. Security CONOPS. The security CONOPS provides a detailed description of system input, system processing, and intermittent and final outputs. Descriptions of all interactions and connections with external systems must be included. Use of diagrams, maps, pictures, and tables are encouraged. This section must be understandable by non-technical managers.

1.2.5.4. Security Policy. The C&A team may chose to add this optional section. In general terms, this section states what is and is not permitted in the field of security during the general operation of the system. The security policy section describes the exceptions to the policies contained in the laws, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. This section establishes policy precedence when more than one policy applies. A list of polices that apply to the system is provided. The purpose of this section is to develop mission-level security objectives through deductive reasoning. Security objectives are the top most level of specifications and focus on the security related aspects of the identified mission. Security objectives must be concise, declarative sentences derived from analysis of mission information, threat, and umbrella security guidance. These security objectives should be written in terms that are independent of architecture and implementation. Each security objective should be justified by rationale. The rationale documents the mission objectives supported by that security objective, the threat driving the security objective, the consequences of not implementing the objective, and applicable umbrella security guidance supporting that security objective. The rationale binds each security objective to a mission objective and focuses attention on security at the mission level.

1.2.5.5. Network connection rules. If the system is to be connected to any other network or system, there may be additional requirements incurred by connection to that system. For example, the DISA DAA for SIPRNet has defined connection requirements for all systems to be connected to the SIPRNet. These impose additional security requirements that must be evaluated in the C&A. These

requirements and those of other systems that may be connected to this system or network must be added to this section.

1.2.5.6. Configuration and change management requirements. This section should reference the system owner's or PM's organizational regulations or instructions regarding the review and approval of modifications or changes to the system. Configuration management policy or Configuration Management Review Board charter requirements must also be included. The requirements should be added to the RTM.

1.2.5.7. Reaccreditation Requirements. Similar to the configuration management requirements, there may be unique organizational requirements related to the reaccredidation or reaffirmation of the approval to operate. These requirements must be referenced in this section and added to the RTM.

1.2.6. Organizations and Resources. The organization description must describe the organization responsible for ensuring compliance with the SSAA. A chart may be used. This section will address issues of staffing, training, and support needs. Chapter 3, Task 1-7 provides additional guidance on the preparation of this section.

1.2.6.1. Identification of Organizations. Describe the organization responsible for ensuring compliance with the SSAA and list the roles and responsibilities of all participants, including the DAA, CA, user representative, ISSO, and any other organizations that may be needed to support the C&A effort.

1.2.6.2. Resources. This section should provide a description of the personnel staffing requirements.

1.2.6.3. Training for the Certification Team. This section describes the training requirements, types of training, who is responsible for preparing and conducting the training, equipment that will be required to conduct training, and training devices that must be developed to accomplish training.

1.2.7. DITSCAP Plan. The plan documents the level of certification analysis, the tasks and milestones, the schedule, the level of effort, and the roles and responsibilities. The section provides the vehicle to develop a mutual understanding of the system among organizations.

1.2.7.1. Tasks and Milestones. The tasks and milestones detail security-related functions, schedules, estimated duration, responsible activity, and completion criteria. The considerations, detailed information on activities, and tradeoffs are associated with each list item.

1.2.7.2. Schedule Summary. The schedule of security activities is a calendar of the certification analysis and other events that lead to an accreditation schedule. This information is presented in chronological sequence and details the development and current status of the agreement. The schedule contains information similar to the tasks and milestones but in time order for scheduling.

1.2.7.3. Level of Effort. Section 4.9 of the SSAA specifies the level of certification analysis. The security classes are used to derive the certification analysis levels. The certification analysis ensures that the appropriate security solutions are defined and the level of effort required to execute the certification activity is specified. For other activities, negotiated and planned levels of effort are recorded in this section.

1.2.7.4. Roles and Responsibilities. This section details the responsibilities and identities of the persons and organizations responsible for the development, execution, maintenance, and evaluation of the SSAA.

1.2.8. Appendices.

1.2.8.1. Certification Results. This section contains all formal test and analysis results, memorandum of agreement (MOA), memorandum of understanding (MOU), accreditation approval, and the authorization to operate.

1.2.8.2. Risk Assessment Results. This section includes an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

1.2.8.3. Contingency Plan(s). This section should describe the emergency responses, backup procedures, backup operations, recovery, and emergency destruction of classified data. The detail of the contingency plan is influenced by the IT environment, the criticality of the functional applications being supported and the user's requirements.

1.2.8.4. System Development Artifacts or System Documentation. This section contains a list of appropriate system development documentation as developed. It specifies the availability and source of the documentation. For example, the change management control procedures may be included in this section. These procedures should identify and document the functional and physical characteristics of the system, control changes to those characteristics, and record and report change processing and implementation status.

1.2.8.5. Accreditation Documentation and Accreditation Decision. This section contains the authorization to operate in a formal memorandum from the DAA to the acquisition agency.

_____
_____

Certification Agent Signature/Date
(User Representative

APPENDIX F

FOR USE AS SAMPLE ONLY

To complete your SSAA, you must obtain a copy of the DoD Instruction 5200.40 and the associated DITSCAP Application Document (DoD 5200.40-M).

SYSTEM SECUITY AUTHORIZATION AGREEMENT (SSAA)

FOR

Enterprise Information Systems Configuration (EISC)

ANY OFFICE

Fort Army, USA

MAY 1999

_____
_____

(DAA Signature/Date)
(System Manager Signature/Date

ANY OFFICE – SSAA

TABLE OF CONTENTS

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION.

1.1. System Name and Identification. This System Security Authorization Agreement (SSAA) is being developed by the ANY OFFICE, Ft. Army, USA in support of operating its enterprise information systems configuration (EISC), hereafter referred to as the ANY OFFICE EISC. The ANY OFFICE is a tenant activity on the Ft. Army installation.

1.2. System Description. The ANY OFFICE EISC consists of a router; a server; four workstations with associated printers, and a laptop computer. The four workstations and server are interconnected to form a local area network (LAN). The LAN server is connected to the ANY OFFICE router that in turn is directly connected to a router on the Ft. Army, USA installation wide area network (WAN). Connectivity to the Ft. Army, USA WAN supports access to the Ft. Army network, the NIPRNET, and the broader Internet. The four workstations are configured to share information while connected to the LAN. The laptop is used in remote locations and, if necessary, may be added as a direct connect workstation to the LAN. The laptop and, when necessary, any of the four workstations may be used with a modem to dial directly into a remote system under the following circumstances:

when the user and laptop are at a remote location

when the remote device to which connectivity is required does not support network connection protocols, or

when the office network connection via the LAN becomes unavailable.

A diagram showing the ANY OFFICE EISC concept of operations and communications connectivity described above is at Appendix A.

1.3. Functional Description.

1.3.1. System Capabilities. The ANY OFFICE EISC is used to provide those services traditionally found in the office environment, e.g., text editing, spreadsheet, database management, graphics, web browsing, electronic mail, etc. In addition, connectivity is required to the Ft. Army, USA WAN for interactive sessions with other resources connected to the WAN, the NIPRNET, and the broader Internet.

1.3.2 System Criticality. The criticality of the ANY OFFICE EISC is of the nature that its availability and use is important to the internal operations of the ANY OFFICE, but if for any reason the EISC becomes unavailable, that unavailability would have no significant adverse affect on Army operations.

1.3.3. Classification and Sensitivity of Data Processed. Sensitive But Unclassified (SBU) information will be processed, stored, and transmitted on/via the ANY OFFICE EISC.

1.3.4. System User Description and Clearance Levels. All personnel within the ANY OFFICE are authorized access to SBU information.

1.3.5. Life-Cycle of the System. The ANY OFFICE EISC is comprised of commercial off the shelf (COTS) hardware and software and is in the operation and maintenance phase of the life cycle process. The expected life cycle use of the

existing components in this configuration is a minimum of two years. As required, additional COTS equipment may be acquired and integrated into the configuration or used to replace existing components.

1.3.6. TCSEC/Common Criteria. The following information is provided with respect to the levels of trust associated with the various components of the ANY OFFICE EISC:

Router – dedicated security processing mode.

Server – dedicated security processing mode.

All Workstations (includes laptop(s)) – dedicated security processing mode.

1.4. System CONOPS Summary. The ANY OFFICE EISC provides office personnel with those services traditionally found in the office environment and gives them the capability to have interactive sessions with other resources on the broader Internet as a result of its network connectivity to the Ft. Army, USA WAN. The use of either the laptop or a workstation with a modem gives the ANY OFFICE personnel the capability to access remote systems when the user is in a remote location; when the remote system does not support connectivity via network protocols; or from the office should the network connection via the LAN not be available. The ANY OFFICE EISC does not jointly perform any security functions with other information systems outside the ANY OFFICE enclave.

2. ENVIRONMENT DESCRIPTION.

2.1. Operating Environment. The ANY OFFICE EISC is physically located in Building 1, Room 122, Fort Army, USA. Physical security countermeasures in effect within the ANY OFFICE include barred windows and the use of locks on doors and windows to secure the office during non-duty hours. In support of environmental security measures the office is equipped with hand held fire extinguishers. During duty hours, when unattended, and during non-duty hours, the office is locked in support of preventing theft, vandalism, and unauthorized physical access to office resources.

2.2. Software Development and Maintenance Environment. The executive software and application software in use within the ANY OFFICE are COTS products. The ANY OFFICE has no control over the development and maintenance environments for these products. As such, the products are considered to be developed in an open environment although there is some degree of expectancy that the vendors responsible for developing and maintaining the products have exercised and employed good standard business practices and configuration control/management in the product's development and maintenance.

2.3. Threat Description. A generic threat statement in support of this concept of operations is at Appendix B.

3.0. SYSTEM ARCHITECTURAL DESCRIPTION.

3.1. Hardware. All hardware components comprising the ANY OFFICE EISC are COTS products. A list of the hardware environments in use will be maintained at Appendix C.

3.2. Software. Executive software and application software in use on the ANY OFFICE EISC are COTS products. A list of the software environments in use will be maintained at Appendix C.

3.3. Firmware. Firmware (e.g., PROM or EPROM), if any, in use within the components comprising the ANY OFFICE EISC would be a COTS product. The presence or absence of any such firmware in support of operating a component is at the discretion of the manufacturer of the component. Since the products in use within the ANY OFFICE EISC are COTS, the presence of any firmware in the components in use is presumed necessary for the proper operation of the equipment. As such, identifying or attempting to identify these items is not required in support of this certification and accreditation effort.

3.4. System interfaces and external connections. All internal and external communications interfaces are depicted at Appendix A. The communications lines (Thin/Coax) interconnecting the ANY OFFICE router, server, and end user workstations are physically contained within Room 122. Externally, the ANY OFFICE EISC interfaces to the Ft. Army, USA WAN. The communications line connecting the ANY OFFICE router to the Ft. Army, USA WAN router is physically contained within Building 1. No encryption techniques are being employed in support of connecting the components internally or externally, however, an end-to-end 128 bit encryption capability is available at the application level within the internet browser in use at the end user workstation. This encryption capability is used to establish protected communications sessions when connecting to Web Servers that require a secure connection. As end to end encryption capabilities become available in other applications, e.g., the Defense Message System, the ANY OFFICE expects to use and take advantage of these capabilities.

3.5. Data flow (including data flow diagrams). The only external communications interface, see Appendix A, from the ANY OFFICE enclave is its connection to the Ft. Army, USA WAN. This connection provides ANY OFFICE personnel the capability to communicate with Government and non-Government entities via email and provides them with the capability to connect to and access remote hosts and servers connected to the broader Internet for work related purposes. A specific data flow diagram for this concept of operations is not needed.

3.6. TAFIM DGSA, Security View. The ANY OFFICE EISC is located in the military (.mil) domain and will be in consonance with the Defense Goal Security Architecture (DGSA).

3.7. Accreditation Boundary. The accreditation boundary for the ANY OFFICE EISC is depicted at Appendix A. Specifically, this boundary includes only those components (router, server, and workstations) that are controlled, managed, and administered by ANY OFFICE personnel. The accreditation boundary does not include the Ft. Army, USA WAN router as it is not controlled, managed, or administered by ANY OFFICE personnel.

4. ITSEC SYSTEM CLASS. The ANY OFFICE EISC ITSEC system class is used to determine the certification level to be employed in support of the certification and accreditation process. Table D-1, Appendix D, depicts the characteristics and the assigned values used in determining the ANY OFFICE EISC ITSEC system class. Characteristics include the following:

4.1. Interfacing Mode. See Appendix D.

4.2. Processing Mode. See Appendix D.

4.3. Attribution Mode. See Appendix D.

4.4. Mission-related Factor. See Appendix D.

4.5. Accessibility Factor. See Appendix D.

4.6. Accuracy Factor. See Appendix D.

4.7. Information Categories. See Appendix D.

4.8. System Class Level. As depicted by Table D-1 at Appendix D, the below system class characteristics for the ANY OFFICE EISC have been derived from the factors assigned to the above modes, factors, and categories in the areas of operation, data, and infrastructure:

Interfacing Mode - Active

Processing Mode - Dedicated

Attribution Mode - Rudimentary

Mission-Reliance Factor - Partial

Accessibility Factor - Reasonable

Accuracy Factor – Approximate

Information Categories - Sensitive

4.9. Certification Analysis Level.

4.9.1. Verification Phase. As derived from information depicted in Tables E-1 and E-2 at Appendix E, the Certification Analysis Level required for the ANY OFFICE EISC is Level 2. Level 2 tasks that are to be completed for certification analysis of the ANY OFFICE EISC during the Verification Phase of this effort are outlined at Appendix F. These tasks were extracted from the Draft DoD 5200.40-M, DITSCAP Application Document, Dec 98 and have been tailored to fit this certification and accreditation effort. Results from completing these tasks will be documented.

4.9.2. Validation Phase. Certification tasks that are to be completed on the ANY OFFICE EISC during the Validation Phase of this effort are outlined at Appendix G. These tasks were extracted from the Draft DoD 5200.40-M, DITSCAP Application Document, Dec 98 and tailored to fit this certification and accreditation effort. Results from completing these tasks will be documented and form the basis for the Certification Authority's recommendation.

5. SYSTEM SECURITY REQUIREMENTS.

5.1. National/DoD/Army Security Requirements. AR 380-19, Information Systems Security, 27 Feb 98 was used to

determine these security requirements. Technical and non-technical security requirements for the ANY OFFICE EISC are outlined at Appendix H.

5.2. Governing Security Requisites. Neither the ANY OFFICE; ANY OFFICE HIGHER HEADQUARTERS; nor the Designated Approving Authority (DAA) for operation of the ANY OFFICE EISC have stipulated any additional security requirements to those derived from AR 380-19 and outlined in Appendix H.

5.3. Data Security Requirements. Neither the ANY OFFICE; ANY OFFICE HIGHER HEADQUARTERS; nor the Designated Approving Authority (DAA) operation of the ANY OFFICE EISC have stipulated any additional security requirements to those derived from AR 380-19 and outlined in Appendix H.

5.4. Security CONOPS. Appendix A is a diagram that depicts the concept of operations for using the ANY OFFICE EISC. From a high level perspective, the Security CONOPS for the ANY OFFICE EISC as it relates to the diagram includes the following:

using the ANY OFFICE EISC router operating system software to enforce access control to the router itself.

using the ANY OFFICE EISC router as firewall between the ANY OFFICE LAN and the Ft. Army USA WAN.

using the ANY OFFICE LAN server operating system to enforce access control on administrator and user accounts on the server.

leveraging the use, when possible, of end to end encryption services integrated into applications, e.g., web browsers, installed on ANY OFFICE EISC end user workstations (includes laptop computers).

leveraging the use of anti-viral software to mitigate and prevent the affects of known viruses and other malicious code programs.

5.5. Security Policy. The following are also required in support of satisfying the verification, validation, and Post Accreditation Phases of the certification and accreditation process:

5.5.1. ISSO Appointment Orders. The orders appoint the individual(s) assigned as the ISSO(s) for the ANY OFFICE EISCA.

5.5.2. Standing Operating Procedures. Administrative procedures and security policy and procedures to be followed locally by all personnel assigned to the ANY OFFICE will be outlined in the ANY OFFICE Standing Operating Procedures (SOP).

5.5.3. Technical Security Configuration of Devices Enforcing a Security Policy. Operational and security configurations enforcing a security policy on the ANY OFFICE router and LAN server will be documented in the ANY OFFICE Technical Security Configuration of Devices Enforcing a Security Policy.

5.5.4. Waivers. A waiver from proper authority will be obtained when an exception to any Army security regulation is required.

5.6. Network Connection Rules.

5.6.1. To Connect to This System. Not applicable, as the ANY OFFICE EISC is not a communications backbone or a wide area network service provider. The ANY OFFICE LAN server is used as a file server and email server for office personnel who are authorized access to the server.

5.6.2. To Connect to Other Systems Defined in the CONOPS. The Ft. Army, USA WAN network manager requires a copy of the ANY OFFICE EISC Accreditation Statement and a copy of Appendix A in support of providing network connectivity to the ANY OFFICE enclave.

5.7. Configuration and Change Management Requirements. Procedures for making changes to existing hardware and software in use within the office environment and for integrating additional or replacement information technology into the office environment will be outlined in the ANY OFFICE EISC Configuration Management Plan.

5.8. Reaccreditation Requirements. Reaccreditation requirements will be addressed in the approval statement issued for the ANY OFFICE EISC by the DAA from ANY OFFICE HIGHER HEADQUARTERS, Ft. Army, USA.

6. ORGANIZATIONS AND RESOURCES.

6.1. Identification of Organizations.

6.1.1. DAA – Any Body, ANY OFFICE HIGHER HEADQUARTERS, Ft. Army, USA

6.1.2. Certification Authority (CA) – No Body, ANY OFFICE, HIGHER HEADQUARTERS, Ft. Army, USA

6.1.3. Identification of the User Representative – Some Body, ANY OFFICE, Ft. Army, USA

6.1.4. Identification of the Organization Responsible for the System – ANY OFFICE, Building 1, Room 122, Ft. Army, USA

6.1.5. Identification of the Program Manager or System Manager – Pea Body, ANY OFFICE, Ft. Army, USA

6.1.6. Information Systems Security Officer (ISSO) – Anti Body, ANY OFFICE, Ft. Army, USA

6.2. Resources.

6.2.1. Staffing Requirements. The ANY OFFICE ISSO is responsible for ensuring the development of all the documentation necessary to support the certification and accreditation of the ANY OFFICE EISC. The certification test team for the Validation Phase of the will consist of the CA from ANY OFFICE HIGHER HEADQUARTERS and the ANY OFFICE ISSO.

6.2.2. Funding Requirements. Since certification and accreditation activities associated with the ANY OFFICE EISC are being accomplished, in-house, locally and with existing personnel, there are no identified requirements for additional funding.

6.3. Training for the Certification Team. No additional training is required by the CA or the ISSO in order to conduct the certification testing required during the Validation Phase of the ANY OFFICE EISC certification and accreditation effort..

6.4. Roles and Responsibilities. The roles and responsibilities of the Certification Team Members are outlined at Appendix I.

6.5. Other Supporting Organizations or Working Groups. The Certification Team is not augmented with members from any other organizations or working groups.

7. DITSCAP PLAN.

7.1. Tailoring Factors.

7.1.1. Programmatic Considerations. The ANY OFFICE is a tenant activity on the Ft. Army, USA, installation. This office handles routine administrative activities at the SBU level.

7.1.2. Security Environment. The ANY OFFICE security environment was previously addressed in paragraph 2.1 above.

7.1.3. IT System Characteristics. The ANY OFFICE EISC functions and characteristics were previously addressed in paragraph 1.3 above.

7.1.4. Reuse of Previously Approved Solutions. A check of the Defense Information Systems Agency web site for any previously approved solutions which could be leveraged in support of certifying and accrediting the ANY OFFICE EISC met with negative results.

7.1.5. Tailoring Summary. This SSAA documents the tailored approach agreed to by the DAA, the CA, the System Manager, and the User Representative for certifying and accrediting the ANY OFFICE EISC.

7.2. Tasks and Milestones. A task and milestone schedule for completing the certification and accreditation of the ANY OFFICE EISC is at Appendix J.

7.3. Schedule Summary. A schedule of security activities of the certification analysis and other events that lead to accreditation of the ANY OFFICE EISC is at Appendix K.

7.4. Level of Effort. The level of certification analysis required in support of certifying and accrediting the ANY OFFICE EISC is identified in paragraph 4.9, above. No other negotiated or planned levels of effort for any other activities are required in support certifying and accrediting the ANY OFFICE EISC.

7.5. Roles and Responsibilities. The responsibilities and identities of personnel and organizations responsible for the development, execution, maintenance, and evaluation of the SSAA are at Appendix L.

8. APPENDICES. The below listed appendices are currently identified as the minimum required to support the overall certification and accreditation (C&A) process of the ANY OFFICE EISC. While all of the appendices are required, those appendices preceded by an asterisk (*), Appendices A through L, will be completed, included, and approved as part of the initial SSAA during the Definition Phase of the overall C&A process. The appendices not preceded by an asterisk (*) will be completed in support of the Verification and Validation Phases of the overall C&A process and used/followed during the Post Accreditation Phase of the process. The SSAA and all of the appendices identified below collectively become the complete accreditation package and documentation for this effort.

8.1. *APPENDIX A ANY OFFICE EISC Concept of Operations Diagram

8.2. *APPENDIX B ANY OFFICE EISC Threat Statement

8.3. *APPENDIX C ANY OFFICE EISC Hardware/Software Environments

8.4. *APPENDIX D ANY OFFICE EISC ITSEC System Class

8.5. *APPENDIX E ANY OFFICE EISC Certification Analysis Level

8.6. *APPENDIX F ANY OFFICE EISC Verification Phase Certification Tasks

8.7. *APPENDIX G ANY OFFICE EISC Validation Phase Certification Tasks

8.8. *APPENDIX H ANY OFFICE Technical and Non-Technical Security Requirements

8.9. *APPENDIX I ANY OFFICE EISC Certification Team Member Roles and Responsibilities

8.10. *APPENDIX J ANY OFFICE EISC Tasks and Milestones

8.11. *APPENDIX K ANY OFFICE EISC Schedule Summary

8.12. *APPENDIX L ANY OFFICE EISC SSAA Roles and Responsibilities

8.13. APPENDIX M ANY OFFICE ISSO Appointment Orders

8.14. APPENDIX N ANY OFFICE Standing Operating Procedures

8.15. APPENDIX O ANY OFFICE Technical Security Configurations of Devices Enforcing a Security Policy

8.16. APPENDIX P ANY OFFICE EISC Configuration Management Plan

8.17. APPENDIX Q ANY OFFICE EISC Results from Verification Phase Certification Analysis

8.18. APPENDIX R ANY OFFICE Risk Management Review

8.19. APPENDIX S ANY OFFICE Certification Test Plan/Procedures

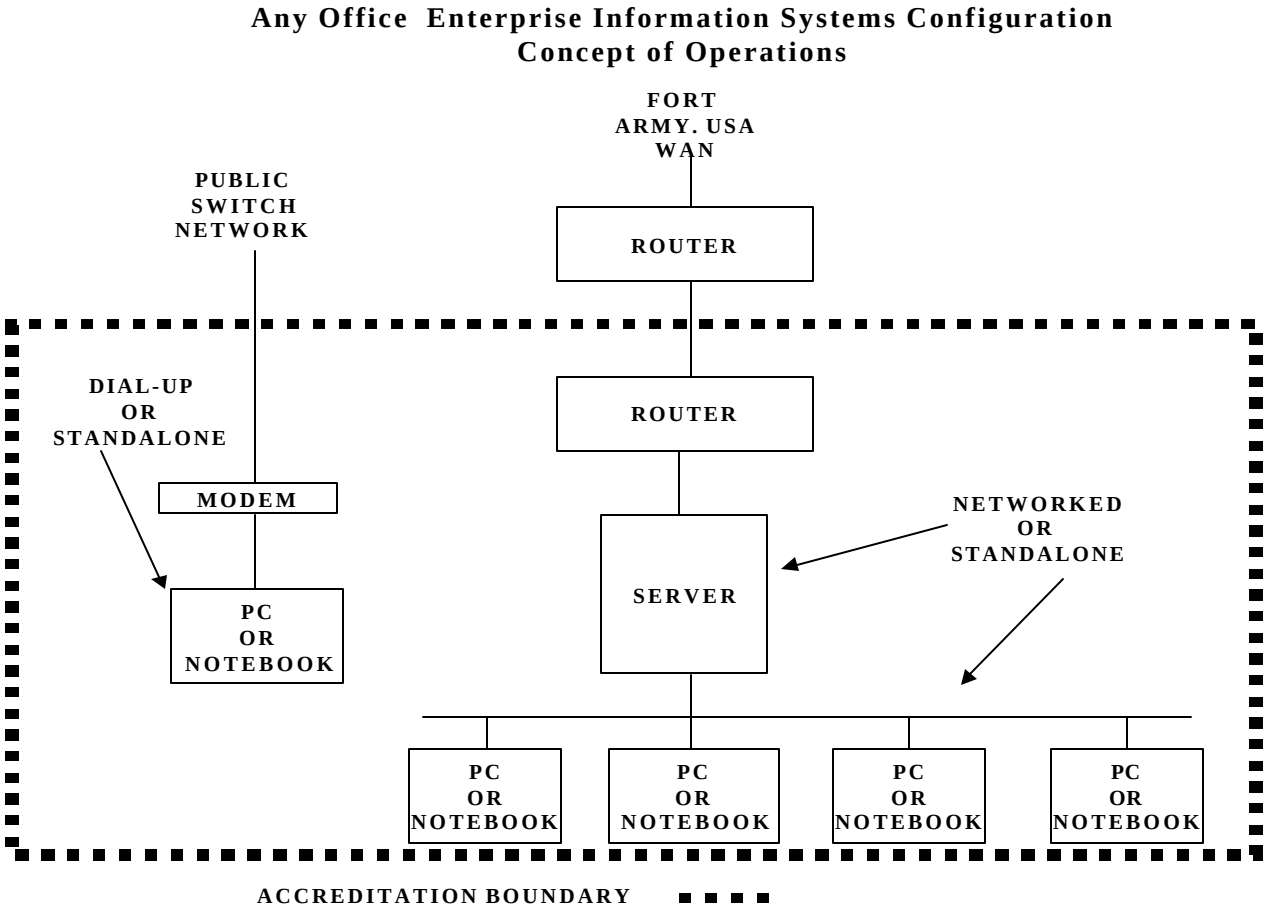
8.20. APPENDIX T ANY OFFICE EISC Certification Results/Recommendation

8.21. APPENDIX U ANY OFFICE Waivers

8.22. APPENDIX V DAA Accreditation Statement for ANY OFFICE EISC

APPENDIX A

ANY OFFICE EISC Concept of Operation
Diagram



APPENDIX B

ANY OFFICE EISC Threat Statement

A system may be subjected to a range of generic threats that are applicable to most commercial and government information systems processing classified or sensitive information. These potential threats could well impact the confidentiality and integrity of the information processed, stored, and transmitted by the system. A potential threat also exists to the availability of the assets of the system which execute mission essential or related processes. Potential threats to the system are from natural and manmade sources. Natural disasters and damage can result from fire, water, wind, and electrical sources. Man-made threats are from those who would target the system for espionage, criminal activity, unlawful use, denial of service, or malicious harm. External or internal agents of threats include espionage services, terrorist, hackers, and vandals.

Statistical analysis of computer-related incidents indicates that the greatest threat to a system is from a trusted agent who has access to that system. The first incident scenario involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the system, one of its components, or information processed, stored, or transmitted by the system. The second incident scenario involves an authorized user who takes deliberate action to damage the system, one of its components, or its data for personal gain or vengeful reasons. Such a person could also engage in espionage, other criminal activity, or exploitation or expropriation of the assets of the system for personal gain. Another incident scenario involves the co-option of users with authorized access to the system, contractor support personnel, or employees with physical access to the system components arising with the motivation of financial gain.

Disgruntled employees pose another threat, especially those who are to be terminated for cause. The most common threat is that posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of unauthorized software or data. Finally, there is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data arising due to failure of users to be properly trained in the use and operation of the system.

These insider threats can be manifested in the following ways:

-- The unauthorized reading, copying or disclosure of sensitive information,

-- The execution of denial of services attacks,

-- The introduction into the system of viruses, worms or other malicious software,

-- The destruction or corruption of data (intentional or unintentional),

-- The exposure of sensitive data to compromise through the improper labeling or handling of printed output, or

-- The improper labeling or handling of magnetic media resulting in the compromise of sensitive information.

The co-opted insider would most likely copy to disk and remove from the system any types of sensitive information to which such a user had authorized access. Such a user might also probe the system in an attempt to discover ways to circumvent access permissions and copy and remove from the

system sensitive information to which such a user did not have authorized access. This might be attempted by an extremely sophisticated user or hacker (or by someone that is under the direction and control of such a person). The individual might be attempting to discover ways to introduce a software sniffer into the system to learn the user ID and password of a system administrator or other privileged user. By masquerading as such a user the individual could bypass access controls and gain access to the most sensitive information on the system. In instances of these types of attacks, there could well be attempts to gain unauthorized access to and modify audit data in order to prevent analysis and detection of the source and nature of the attack. It goes without saying, that the most serious of all types of possible attacks against the system could be mounted by co-opted systems administration personnel, with their ability to alter or bypass most, if not all, of the system's protection mechanisms.

APPENDIX C

PLACE MARK FOR ANY OFFICE EISC
Hardware/Software Environments

APPENDIX D

ANY OFFICE EISC ITSEC System Class

Characteristic	Operation	Data	Infrastructure	System	Alternatives
Interfacing Mode	Active	Active	Active	Active	Benign, Passive, or Active
Processing Mode	Dedicated	Dedicated	Dedicated	Dedicated	Dedicated Level, Compartmented Level, System High, or Multilevel
Attribution Mode	Rudiment-ary	Rudiment-ary	Rudiment-ary	Rudiment-ary	None, Rudimentary, Basic, or Comprehensive
Mission-Reliance Factor	Partial	Partial	Partial	Partial	None, Cursory, Partial, or Total
Accessibility Factor	Reason-able	Reason-able	Reason-able	Reason-able	Reasonable, Soon, ASAP, or Immediate
Accuracy Factor	Approxi-mate	Approxi-mate	Aproxi-mate	Approxi-mate	Not-applicable, Approximate, or Exact
Information Categories	Sensitive	Sensitive	Sensitive	Sensitive	Unclassified, Sensitive (Privacy Act, Financially Sensitive, Administrative, Proprietary, or Other), Collateral Classified, or Compartmented/Special Access Classified

Table D-1 ANY OFFICE EISC ITSEC Class Characteristics.

APPENDIX E

ANY OFFICE EISC Certification Analysis Level

Characteristics	System Selection Alternaive Values	ANY OFFICE EISC System Values	Assigned Weight =
Interfacing Mode	Benign (w=0), Passive (w=2), Active (w=6)	ACTIVE	6
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented Level (w=5), Multi-level (w=8)	DEDICATED	1
Attribution Mode	None (w=0), Rudimentary (w=1), Basic (w=3), Comprehensive (w=6)	RUDIMENTARY	1
Mission-Reliance Factor	None (w=0), Cursory (w=1), Partial (w=3), Total (w=7)	PARTIAL	3
Accessibility Factor	Reasonable (w=1), Soon (w=2), ASAP (w=4), Immediate (w=7)	REASONABLE	1
Accuracy Factor	Not-applicable w=0), Approximate (w=3), Exact (w=6)	APPROXIMATE	3
Information Categories	Unclassified (w=1), Sensitive (w=2), Collateral Classified (w=6), Compartmented or Special Access Classified (w=9)	SENSITIVE	2
	TOTAL OF ALL WEIGHTS		17

TABLE E-1

ANY OFFICE System Characteristics/Levels and Total of Assigned Weights

CERTIFICATION LEVEL	WEIGHT	ANY OFFICE EISC DETERMINED WEIGHT	ANY OFFICE EISC CERTIFICATION LEVEL
Level 1	< 16		
Level 2	12 – 32	17 (Value From Table Above)	X
Level 3	24 – 44		
Level 4	38 - 50		

TABLE E-2
ANY OFFICE Certification Level Determination

APPENDIX F
PLACE MARK ANY OFFICE EISC Verification Phase Certification Tasks

APPENDIX G
PLACE MARK ANY OFFICE EISC Validation Phase Certification Tasks

APPENDIX H
PLACE MARK FOR ANY OFFICE Technical and Non-Technical Security Requirements

APPENDIX I
PLACE MARK FOR ANY OFFICE EISC Certification Team Member Roles and Responsibilities

APPENDIX J
PLACE MARK FOR ANY OFFICE EISC Tasks and Milestones

APPENDIX K
PLACE MARK FOR ANY OFFICE EISC Schedule Summary

APPENDIX L
PLACE MARK FOR ANY OFFICE EISC SSAA Roles and Responsibilities

PPENDIX M

PLACE MARK FOR ANY OFFICE ISSO Appointment Orders

APPENDIX N

PLACE MARK FOR ANY OFFICE Standing Operating Procedures

APPENDIX O

PLACE MARK FOR ANY OFFICE Technical Security Configuration of Devices Enforcing a Security Policy

APPENDIX P

PLACE MARK FOR ANY OFFICE EISC Configuration Management Plan

APPENDIX Q

PLACE MARK FOR ANY OFFICE EISC Results from Verification Phase Certification Analysis

APPENDIX R

PLACE MARK FOR ANY OFFICE Risk Management Review

APPENDIX S

PLACE MARK FOR ANY OFFICE Certification Test Plan/Procedures

APPENDIX T

PLACE MARK FOR ANY OFFICE EISC Certification Results/Recommendation

APPENDIX U

PLACE MARK FOR ANY OFFICE Waivers

APPENDIX V

PLACE MARK FOR DAA Accreditation Statement

Appendix G --Example VULNERABILITIES

1. PHYSICAL SECURITY VULNERABILITIES

Inadequate Equipment Protection: The system equipment is not adequately protected against probing, substitution, or theft (e.g., system equipment is not located in secure areas).

Inadequate Protection Against Loss of Power: The system does not have adequate access to power generation facilities or backup power supplies and does not have adequate protection of system information and components in the event of main power loss.

Inadequate Protection Against Power Surges/Spikes: The system fails to provide protection against power surges and voltage spikes on any incoming power lines.

Inadequate Heating, Ventilation, and Air Conditioning: The operational environment of the system does not adequately remain within the specified operational temperatures.

Inadequate Protection Against Natural Disaster: The system is not installed in an environment that will adequately protect it in the event of a natural disaster.

Inadequate EMI Protection: The system does not adequately protect electronic components and information from Electro-Magnetic Interference.

2. PERSONNEL SECURITY VULNERABILITIES

Login: An unauthorized person has the ability to bypass or subvert the login mechanism.

Access Controls: An authorized or unauthorized person has access to, and the ability to use system functions or information for which permissions have not been granted.

Inadequate Operator Warning for Execution of Critical Functions: The system fails to warn the operator upon initiation of a critical function that the execution of that function could lead to system failure, degradation, or have security-related significance.

3. ADMINISTRATIVE SECURITY VULNERABILITIES

Lack of Communications Backup Mechanisms: The system does not provide adequate backup mechanisms in the event that the primary communication resources are inoperable.

Inadequate Compromise Recovery Mechanism: The system does not provide adequate compromise recovery mechanisms for the retrieval of compromised information.

4. MEDIA SECURITY VULNERABILITIES

Inadequate Security Highlighting: The system fails to adequately indicate the security level of the information being displayed on a terminal.

Inadequate Security Labeling of Printed Output: The system fails to adequately label printed output with the appropriate security level.

Lack of Disk/Magnetic Media Erasure: The system fails to ensure the erasure of the data stored on disks and other magnetic media after the media memory has been deallocated and prior to initial allocation or reallocation.

5. EMANATIONS SECURITY VULNERABILITIES

Use of Non-TEMPEST-approved Equipment: The system contains equipment that does not meet TEMPEST requirements imposed on that equipment.

6. COMPUTER SECURITY VULNERABILITIES

Inadequate Recording of Security-Relevant System Events: The system fails to record security-related system and network events to the security audit file.

Inadequate Recording of Security-Relevant Event-Specific Information: The system fails to record security-related event information into an audit file (e.g., operator ID, terminal ID, time of event, date of event).

Inadequate Audit Protection: The system fails to adequately protect the audit log against inadvertent or malicious modification, disclosure, and deletion.

Inadequate Management of Audit Data: The system fails to provide adequate procedures or mechanisms for archiving, retrieving, and reviewing audit data.

Inadequate User Identification and Authentication Mechanisms: The system fails to provide mechanisms that ensure each operator is uniquely identifiable by the system and the system fails to adequately verify the identity of the operator (e.g., through password mechanisms, biometrics, or other authentication devices).

Inadequate Device Identification and Authentication Mechanisms: The system fails to provide mechanisms that ensure each hardware device is uniquely identifiable by the system and the system fails to adequately verify the identity of the device (e.g., through PROMs in the device).

Lack of Password Suppression During Entry: The system fails to suppress the display of the password.

Lack of Minimum Password Length/Content Enforcement: The system fails to reject and notify personnel of passwords that are shorter than the predefined minimum password length or fail to meet predefined content requirements.

Lack of Password Expiration Mechanism: The system fails to retire passwords that have remained on the system longer than a predefined maximum password life.

Lack of Password Replacement Mechanism: The system fails to force authorized users to replace passwords that have expired or been compromised, and/or fails to allow authorized users to change their password at any time.

Lack of Provision of Last Login Information: The system fails to provide the user with the time and date of the last login attempt for the specific user id. The system also fails to indicate if the last login attempt was successful or not.

Inadequate Audit of Modifications: The audit log fails to adequately record changes made and changes occurring in the system (e.g., tracking and review of HW/FW/SW modifications).

Lack of Workstation Time-out Capability: The system fails to allow the ability to shut down workstation that have had no operator activity for a pre-determined amount of time.

Lack of Protection Access Control Information: The system fails to adequately protect the access control

information against inadvertent or malicious modification, disclosure, and deletion.

Inadequate Resource Allocation Controls: The system fails to ensure that resources are effectively allocated and protected against resource overload and misappropriation.

Lack of Adequate System Recovery Mechanisms: The system fails to ensure recovery to a known, secure, operational state after a power failure, system failure, or system start-up. In the case of failure, the system must fail to a known state so as not to compromise data.

Lack of Hardware Redundancy: The system does not provide duplicity for hardware performing critical functions in the event that one or more of the devices is no longer operable.

Inadequate Access Control Mechanisms: The system fails to ensure appropriate assignment of system permissions to system personnel. The system fails to ensure that only the necessary tools and information for an operator to accomplish a task will be allowed to be accessed by that operator. The system fails to protect system processes from access by unauthorized operators. The system fails to adequately protect maintenance processes from access by unauthorized operators (e.g., OS command line, compilers, and/or debuggers).

Lack of Differentiated Operator Permission Levels: The system fails to differentiate between different system access levels (e.g., Administrator, System Operator, System Maintainer).

Inadequate Verification of System Permissions: The system fails to ensure verification of the operator's system permissions prior to allowing the requested access.

Inadequate R/W/E/D File Mechanisms: The system fails to provide adequate file management tools for the manipulation and execution of system files.

Lack of Network Server Memory Erasure: The system fails to ensure the erasure of system main memory after the memory has been deallocated and prior to initial allocation or reallocation.

Lack of Workstation Memory Erasure: The system fails to ensure the erasure of the workstation memory after the memory has been deallocated and prior to initial allocation or reallocation.

Inadequate Virus Screening Mechanisms: The system fails to provide adequate virus screening mechanisms during development, before installation, and during use, to keep viruses from gaining access to the system and to eliminate them in the event that they do gain access to the system.

Inadequate Software/Data Integrity Mechanisms: The system fails to provide integrity mechanisms (e.g., checksums) to ensure the secure and uncorrupted transfer and storage of software and data.

Inadequate Message Recovery Mechanisms: The system fails to provide adequate recovery mechanisms for the loss of system and user information.

Inadequate Protection of Security Mechanisms: System mechanisms that provide security to the system are not adequately protected from destruction and/or corruption.

Inadequate Detection and Reporting of HW/FW/SW Errors: The system fails to provide adequate mechanisms to run diagnostics automatically or, fails to allow an authorized user to run diagnostics when necessary (e.g., detection and reporting of HW/FW/SW errors).

Inadequate Separation of Information Between Communities of Interest: The system fails to ensure the separation of user data and control information.

7. COMMUNICATION SECURITY

Lack of Workstation/User Account Lockout Capability: The system fails to provide a means to lockout communications to and from a specified workstation.

Inadequate Protection of Authentication Data During Transmission: The system fails to adequately protect remote user authentication data from modification, deletion, or disclosure.

Use of Unprotected Communication Circuits: Unencrypted classified or sensitive information is transmitted across either intra-system communication lines, radio frequency communication channels, or wire line.

Unauthorized Bypass of Cryptographic Equipment: Unauthorized classified or sensitive information is bypassed around the cryptographic equipment (e.g., misuse of trusted software in the cryptographic equipment).

Lack of Error Detection and Recovery: The system fails to adequately detect and report errors in transmission and/or correct message stream errors.

Use of Unapproved Cryptographic Equipment: Cryptographic traffic and key management algorithms are not approved by NSA for the level of secure traffic being protected.

Inadequate Key Management Mechanisms: The system fails to adequately protect the key and/or has inadequate key distribution/generation/zeroize mechanisms.

Appendix H. Threat Examples

1. Compromising Emanations

Compromising emanations are unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, may disclose the information transmission received, handled, or otherwise processed by any information processing equipment. Compromising emanations (emissions) can be picked up from IS equipment and can reveal classified information. This section discusses the risks associated with compromising emanations.

2. Covert Channels

Two kinds of covert channels, timing and storage, can be threats to the IS. Covert storage channels include all vehicles that would allow the direct or indirect writing of a storage location by one process and the direct or indirect reading of it by another. Covert timing channels include all vehicles that would allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information. This section discusses the risks associated with covert channels.

3. Compromise of Crypto Key

Crypto Key is the key used in the encryption and decryption of data traffic. These keys are highly sensitive and should be highly protected. This section discusses the risks associated with the compromise of cryptographic keys.

4. Data Corruption

Malicious modification of files, alteration of data because of hardware or software failure, and two or more users writing to a file or database simultaneously are examples of data corruption. Data corruption can cause damage to an IS's mission. This section discusses the risks associated with data corruption.

5. Data Loss

Data loss is defined as deletion of data, whether accidental or deliberate. Database files and user data files are included in data loss. This data does not include application programs or system software. Data can be lost through user activity or even computer programming commands. It is possible that a computer program could provide the wrong command to another program, causing data to be overwritten. This section discusses the risks associated with data corruption.

6. Denial of Service

During denial of service, users are unable to use the IS. Denial of service can be caused accidentally or deliberately. Equipment failure may result in the denial of service to only a few users or to an entire IS. This section discusses the risks associated with denial of service.

7. Eavesdropping

Eavesdropping is generally regarded as tapping the communications lines of a computer system. Eavesdropping can be accomplished via telecommunications channels. This section discusses the risks associated with eavesdropping.

8. Equipment Damage

Equipment damage is any damage to equipment, whether accidental or deliberate. Equipment damage can be caused by humans or acts of God. This section discusses the

risks associated with equipment damage.

9. Hacker Penetration

A hacker penetration is defined as the act of any person who has gained unauthorized access to an IS through illegal means. This type of penetration does not always intend to cause harm to the IS, yet can be very dangerous. This section discusses the risks associated with hacker penetration.

10. Hardware Implant

Hardware implants can be added to IS hardware. These implants could impart damage to the IS by causing it to behave in a way that is inconsistent with its mission. This section discusses the risks associated with hardware implant.

11. Hardware Theft

The act of stealing hardware is considered hardware theft. Disk packs, if stolen, may provide a perpetrator with classified information. A special hardware device, perhaps designed for a specific or unique use, could prove beneficial to a perpetrator. This section discusses the risks associated with hardware theft.

12. Knowledgeable Individuals

Knowledgeable individuals comprise IS users. These individuals include not only the system management and operations personnel, but also the regular IS user. Individuals' knowledge to be exploited could be of a sensitive program or project, or how to implement the IS's security features. This section discusses the risks associated with knowledgeable individuals.

13. Misdelivered Data

Misdelivered data includes any data received by a user or device that is not cleared for, does not have formal access to, or possess the need-to-know the information received. It is possible that a user could receive output that does not belong to the user, or that for which the user is not cleared. Misdelivered data can be a result of human error, system failure, or malicious activity. This section discusses the risks associated with misdelivered data.

14. Misuse of Network Connectivity

Network connectivity can be used for personal gain. An IS may connect to another IS for remote diagnostics. A user could use that IS's hard disks for storage of personal data. A perpetrator could use illegally-gained network access as a gateway to other ISs. This section discusses the risks associated with misuse of network connectivity.

15. Misuse of Resources

Misuse of resources involves individuals using the IS' resources (hard disks, etc.) to conduct personal business or for other unauthorized purposes. This section discusses the risks associated with misuse of resources.

16. Replay

Replay is defined as the unauthorized repetition of a process or transaction that permits the circumvention of a system’s security measures. (An example of this is the ability to capture in order to replay other authorized users' userids and passwords to use their access rights).

This section discusses the risks associated with replay.

17. Software Corruption

The IS's system software could be corrupted by an individual with system knowledge and system manager privileges. Although the regular IS user may not have access rights to the system software files, a knowledgeable user may have the ability to access and corrupt system software files, causing system downtime or possibly even data erasure. This section discusses the risks associated with software corruption.

18. Software Implant/Trojan Horse

Software implants or trojan horses can be embedded in software. Such anomalies can cause great harm to an IS through data deletion or program malfunction. This section discusses the risks associated with software implant and trojan horses.

19. Software Loss

Software loss is generally the deletion of software, whether intentional or accidental. It can happen through user error, software or hardware error, or malicious activity. This section discusses the risks associated with software loss.

20. Software Theft

Software theft is the act of stealing software. This action can include an employee's "borrowing" a copy of the latest personal computer (PC) software for use on the employee's home computer. It can violate licensing agreements between the software manufacturer and the Agency. It can also cause infringement of U.S. Copyright Law. This section discusses the risks associated with software theft.

21. Spoofing

"Spoofing" primarily threatens the security of the IS's identification and authentication (I&A) mechanism. As an example, a false IS logon screen could be generated by a malicious program for the next user. The next user would input his userid and password, and the malicious program would accept this input after transmitting the fake logon request. That user would receive an error message, and would be logged off. The user would falsely believe that an incorrect userid or password had been given, and simply try again. This section discusses the risks associated with spoofing.

22. Theft or Compromise of non-SCI (Collateral)

Theft or compromise of collateral information may not be as threatening and may not be as sensitive to the Central Intelligence Agency (CIA) and Intelligence Community as SCI information. Collateral includes unclassified and classified information up to Top Secret (and personnel and budgetary data). However, it is still important to indicate that this data is classified (or could be considered unclassified, but sensitive). Bits and pieces of information acquired could eventually provide the whole picture. This section discusses the risks associated with theft or compromise of non-sensitive compartmented information (SCI) (i.e., Collateral information).

23. Theft or Compromise of SCI

Theft of SCI is the act of deliberately stealing data, documents, etc. containing SCI information. Compromise of SCI can be deliberate or accidental. This section discusses the

risks associated with theft or compromise of SCI.

24. Unauthorized Access

Unauthorized access is defined as any unauthorized person, program, etc., receiving access to an IS and its information through use of a pirated userid or other means. This section discusses the risks associated with unauthorized access.

25. Unauthorized Software

Unauthorized software is any software installed on an IS that is not authorized by the IAM, SM, or other approving IS manager. This section discusses the risks associated with unauthorized software.

26. Viral Infection

A viral infection can attack an IS through the introduction of data diskettes into the system or through network connections. Infection can cause data erasure, program malfunction. Viruses can be very dangerous through their ability to spread from IS to IS. This section discusses the risks associated with viral infection.

GLOSSARY

Section I
Abbreviations

AA
Administrative assistant

ACCLAIMS
Army COMSEC Commodity Logistics Accounting Information Management System

ACCO
Army Case Control Office

ACERT
Army Computer Emergency Response Team

ACERT/CC
Army Computer Emergency Response Team/Coordination Center

ACL – Access Control List

ADP
automated data processing

AIAP
army information assurance program (replacement for AISSP, army information systems security program)

AIARP
Army Information Systems Security Resources Program

AIS
Army information system(s)

AMC
Army Materiel Command

AMHS
automated message handling system

AR
Army regulation

ARNG
Army National Guard

ASA(RDA)
Assistant Secretary of the Army for Research, Development and Acquisition

ASSIST
automated systems security incident support team

AUTODIN
automatic digital network

BAS
battlefield automation systems

C2 Protect
command and control protect

C2W
command and control warfare

C4I
command, control, communication and intelligence

CA
Certification Agent; Certification Authority

CAW
Certification Authority Workstation

CCI
controlled cryptographic item

CD
compact disk

CDR USARCMD
Commander, United States Army Reserve Command

CI
counter-intelligence

CID
criminal investigation division

CISS
center for information systems security

CNG
Chief National Guard

COMPUSEC
computer security

COMSEC
communications security

COTS
commercial off-the-shelf

CSE
client server environment

CSE
contractor support element

CM
configuration management

COOP
Continuity of Operations Plan

CSTVRP
computer security technical vulnerability reporting program

DA
Department of the Army

DAA
designated approving authority

DCID
Director, Central Intelligence Directive

DCSINT
Deputy Chief of Staff for Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations and Plans

DDN
defense data network

DES
data encryption standard

DIA
Defense Intelligence Agency

DIAM
Defense Intelligence Agency Manual

DISA
Defense Information Systems Agency

DISA/CISS
Defense Information System Agency/Center for Information System Security

DISC4
Director of Information Systems for Command, Control, Communications, and Computers

DMS
Defense Message System

DSNET3
DoD Secure Network/3

DOD
Department of Defense

DODISS
Department of Defense Intelligence Information Systems

DSSCS
Defense Special Security Communications System

ECP
engineering change proposal

ETPL
endorsed TEMPEST product list

EUCI
endorsed for unclassified cryptographic item

FM
field manual

FOUO
FOR OFFICIAL USE ONLY

FTA/RA
facility TEMPEST assessment/risk analysis

GSA
General Services Agency

GCCS
Global Command and Control System

GOTS
government off-the-shelf

HQDA
Headquarters, Department of the Army

IAA
interconnected accredited AIS

IATO
interim approval to operate

IAW
in accordance with

IA
information assurance

IAM
information assurance manager

IASO
information assurance security officer

IAPM
information assurance program manager

IARP
information assurance resources program

IM
information management

IMA
information mission area

INFOSEC
information security

INSCOM
United States Army Intelligence and Security Command

IO
information operations

IP
internet protocol

IS
information system(s)

IW
information warfare

JCS
Joint Chiefs of Staff

JROC
Joint Requirement Oversight Council

JTA
Joint Technical Architecture

JWICS
Joint Worldwide Intelligence Communication System

LAA
limited access authorization

LAN
local area network

LIWA
Land Information Warfare Activity

MACOM
major command

MAN
Metropolitan area network

MOA
memorandum of agreement

MOU
memorandum of understanding

NATO
North Atlantic Treaty Organization

NCSC
National Computer Security Center

NACSIM
National Communications Security (COMSEC) Information Memorandum

NISAC
National Information Security Assessment Center

NIST
National Institute of Standards and Technology

NOC
Network Operations Center

NSA
National Security Agency

NSA/CSS
National Security Agency/Central Security Services

NSAM
National Security Manual

NSTISSC
National Security Telecommunications and Information Systems Security Committee

OPSEC
operations security

PC
personal computer

PCMCIA
personal computer memory international association

PDS
protected distribution system

PEO
Program Executive Officer

PL
Public Law

PM
program manager/project manager/product manager

PMO
program management officer

PPL
preferred products list

PROM
programmable read only memory

RADIUS
Remote authentication dial-in user system

RDTE
research, development, test and evaluation

RO
Read Only

ROM
read only memory

RW
Read Write

SA
system administrator

SAP
special access program

SAPI
special access program for intelligence

SBA
site based accreditation

SBU
sensitive but unclassified

SCE
service cryptologic element

SCI
sensitive compartmented information

SCIF
sensitive compartmented information facility

SF
standard form

SII
statement of intelligence interest

SIMO
system integration management office

SIOP-ESI
Single Integrated Operational Plan-Extremely Sensitive Information

SIPRNET
secret internet protocol router network

SOP
standing operating procedure

SSA
system security administrator

SSBI
single scope background investigation

SSO
special security officer

STS
single trusted system

TAP
tactics, techniques, and procedures

TCB
trusted computing base

TCO
TEMPEST control officer

TDY
temporary duty

TFTP
Trivial File Transfer Protocol Server

TNOC
Theater Network Operations Center

TRADOC
United States Army Training and Doctrine Command

TS
top secret

TS/SCI

top secret/sensitive compartmented information

UCMJ
uniform code of military justice

USAR
United States Army Reserve

Section II
Terms

Access
(AIS) Ability and means to communicate with (i.e. input to or receive output from), or otherwise make use of any information, resource, or component in an AIS.
(COMSEC) Capability and opportunity to gain knowledge or to alter information or material.

Access control
The process of limiting access to the resources of an AIS only to authorized users, programs, processes, or other systems.

Accountability
(AIS) Property that enables auditing of activities on an AIS to be traced to persons who may then be held responsible for their actions.
(COMSEC) Principle that an individual is responsible for safeguarding and controlling of COMSEC equipment, keying material, and information entrusted to his/her care and is answerable to proper authority for the loss or misuse of that equipment or information.

Accreditation
A formal declaration by a designated approving authority that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Accreditation authority
Synonymous with designated approving authority.

AIS security incident
An occurrence involving classified or SBU information being processed by an AIS where there may be a deviation from the requirements of the governing security regulations; a compromise or unauthorized disclosure of the information occurred or was possible; data or information integrity is in question (e.g., unauthorized modification); or information was made unavailable for a period of time.

WAN
wide area network

WWMCCS
Worldwide Military Command and Control System

Approval to operate
A term which is synonymous with accreditation.

Army Information
Information originated by or concerning the U.S. Army.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Review
The independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Audit trail - Chronological record of system activities to enable the construction and examination of the sequence of events and/or changes in an event. Audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC material.

Authenticate

To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated information system, or establish the validity of a transmitted message.

Authentication
Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Auto-manual system
Programmable, hand-held COMSEC equipment used to perform encoding and decoding functions.

Automated information systems
(See Information System (IS))

Automated tactical system (ATS) – Any AIS that is used for communications, operations, or as a weapon during mobilization, deployment or tactical exercise. An ATS may include but is not limited to data processors, firmware, hardware, peripherals, software or other interconnected components and devices such as radar equipment, global positioning devices, sensors, guidance systems airborne platforms.

Automated weapon systems (AWS) – Any weapons system that utilizes a combination of computer hardware and software, which performs the functions of an automated information system such as collecting, processing, transmitting and displaying information, in its operation.

Automated information systems security
Synonymous with
computer security.

Availability
The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Category
Restrictive label that has been applied to both classified or unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data. Examples include sensitive compartmented information, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special category information only after being granted formal access authorization.

Central computer facility
One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. Central computer facilities are those areas where computer(s), other than personal computer(s), are housed to provide necessary environmental, physical, or other controls.

Certification
Comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Agent
Individual responsible for making a technical judgment of the system's compliance with stated requirements. Identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Certification Authority
(See Certification Agent (CA))

Classified defense information
Official information regarding the national security which has been designated top secret, secret, or confidential in accordance with Executive Order 12356.

Clearing
Removal of data from an AIS, its storage devices, and other peripheral devices with

storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (i.e., through the keyboard). An AIS need not be disconnected from any external network before clearing takes place. Clearing enables a product to be reused within, but not outside of, a secure facility. It does not produce a declassified product by itself, but may be the first step in the declassification process. See purge.

Commercial COMSEC Endorsement Program (CCEP)
Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices.

Communications deception
Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

Communications security (COMSEC)
Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity.

Compartmented mode
AIS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following:
a. Valid security clearance for the most restricted information processed in the system.
b. Formal access approval and signed non-disclosure agreements for that information to which a user is to have access.
c. Valid need-to-know for information to which a user is to have access.

Compromising emanations
Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment (See TEMPEST).

Computer
A machine capable of accepting data, performing calculations on or otherwise manipulating that data, storing it, and producing new data.

Computer facility
Physical resources that include structures or parts of structures that support or house computer resources. The physical area where the equipment is located.

Computer security
Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Confidentiality
Assurance that information is not disclosed to unauthorized entities or processes.

Configuration control
Process of controlling modifications to a telecommunications or automated information systems hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management - The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of an IS, throughout the development and operational life of the system.

Contingency Plan - Also known as the Continuity of Operations Plan (COOP). A

plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Countermeasure – An action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

Controlled access protection
Log-in procedures, audit of security-relevant events, and resource isolation as prescribed for class C2 in the Orange Book.

Controlled cryptographic item
Secure telecommunications or information handling equipment, or associated cryptographic component, is unclassified but governed by a special set of control requirements. Such items are marked CONTROLLED CRYPTOGRAPHIC ITEM or, where space is limited, CCI.

Cryptographic equipment
Equipment that embodies a cryptographic logic.

Cryptographic
Pertaining to, or concerned with, cryptography.

Cryptography
Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptology
The science and activities which deal with hidden, disguised, or encrypted communications.

Cryptosystem
Associated COMSEC items interacting to provide a single means of encryption or decryption.

Data security
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Declassification (of magnetic storage media)
An administrative procedure resulting in a determination that classified information formerly stored on a magnetic medium has been removed or overwritten sufficiently to permit reuse in an unclassified environment.

Dedicated mode
AIS security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:
a. Valid security clearance for all information within the system.
b. Formal access approval and signed non-disclosure agreements for the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).
c. Valid need-to-know for all information contained within the AIS.
When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Degauss
Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

Denial of service
Result of any action or series of actions that prevents any part of a telecommunications or AIS from functioning.

Designated Approving Authority
Official with the authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk.

Digital Signature – An electronic rather than a written signature used by someone to authenticate the identity of a sender of a

message or signer of a document. A digital signature ensures that the content of a message or document is unaltered. Digital signatures can be time-stamped, cannot be imitated by another person, cannot be easily repudiated, and is transportable.

Discretionary Access Control (DAC)-Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

DOD Trusted Computer System Evaluation Criteria
Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into AIS. This document, DoD 5200.28 STD, is frequently referred to as the Orange Book.

DMZ – Demilitarized Zone (DMZ) is a small network or computer host that serves as a "neutral zone" between an internal network and the public network. A DMZ prevents users for obtaining direct access to an internal server that may have business data on it. A DMZ is another approach to the use of a firewall and can act as a proxy server if desired.

Eavesdropping – method used by an unauthorized individual to obtain sensitive information, such as, passwords, data, and procedures performing functions from a network. Eavesdropping techniques include wiretapping, eavesdropping by radio, eavesdropping via auxiliary ports on a terminal, and use of software that monitors packets sent over a network. Vulnerable network programs are telnet and ftp.

Embedded cryptography
Cryptography which is engineered into an equipment or system the basic function of which is not cryptographic. Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed if identifiable as a separate module within the host.

Embedded (computer) system
Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or in part.

Emission security
Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptographic equipment, AIS, and telecommunications systems.

Extranet –is a private network that uses Internet protocols and the public telecommunications system to securely share between select external users. An Extranet requires the use of firewalls, authentication, encryption, and the use of virtual private networks (VPNs) that tunnel through the public network.

File Server
Computer hardware used to provides storage user data and software applications and processing capabilities for user workstations and normally used for the connection and control for the workstations to the Local Area Network (LAN).

Firewall
A system or group of systems that enforces an access control policy between two networks with the properties of allowing only authorized traffic to pass between the networks from inside and outside the controlled environment and is immune to penetration.

Firmware
Software that is permanently stored in a hardware device which allows reading and executing the software, but not writing or modifying it.

Foreign national employees
Non-U.S. citizens who normally reside in the country where employed, though they may not be citizens of that country, and who are employed by the U.S. Government and the Department of the Army.

Formal access approval
Documented approval by a data owner to allow access to a particular category of information.
IAA View –Interconnected Accredited AIS View. If a network consists of previously accredited AIS, a Memorandum of Agreement (MOA) is required between the DAA of each DOD Component AIS and the DAA responsible for the network. The network DAA must ensure that interface restrictions and limitations are observed for connections between DOD Component AIS. In particular, connections between accredited AIS must be consistent with the mode of operation of each AIS, the specific sensitivity level or range of sensitivity levels for which each AIS own and a component will require an external connection to perform a useful is accredited, any additional interface constraints associated with the particular interface device used for the connection, and any other restrictions required by the MOA.

Information System (IS)
Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Information Assurance (IA)
The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. This regulation designates IA as the security discipline which encompasses COMSEC, COMPUSEC, and control of compromising emanations (TEMPEST).

Information Technology (IT) – The hardware, firmware, and software used as a part of the information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and the automatic data processing equipment. IT includes any assembly hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Integrity
The degree of protection for data from intentional or unintentional alteration or misuse.

Intelligence Information
Information collected and maintained in support of U S intelligence Mission.

Internet - A global collaboration of data networks that are connected to each other, using common protocols (e.g., TCP/IP) to provide instant access to an almost indescribable wealth of information and access to computers around the world.

Intranet - Similar to the Internet, but is accessible only by the organization's employees or others with authorization.

IS Security Incident – Any unexplained event that could result in the loss, corruption, and/or the denial of access to data, as well as any event that cannot be easily dismissed or explained as normal operations of the system.

IS Serious Incident – Any event that poses grave danger to the Army's ability to conduct established information operations.

Key
Information (usually a sequence of random or pseudo-random binary digits) used initially to set up and periodically to change the operations performed in crypt-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-measures patterns (e.g.,frequency hopping or spread spectrum), or for producing other key.

Key management
Process by which a key is generated, stored, protected, transferred, loaded, used, and destroyed.

Least Privilege
Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. This also applies system privileges that might not be needed to perform their assigned job.

NOTE: Application of this principle limits the damage that can result from errors, accidental and unauthorized use of an AIS.

Local Area Networks (LAN) – A system which allows microcomputers to share information and resources with a limited (local) area.

Machine cryptosystem
Cryptosystem in which the cryptographic processes are performed by crypt-equipment.

Mainframe
A computer system which is characterized by dedicated operators (beyond the system users); high capacity, distinct storage devices; special environmental considerations; and an identifiable computer room or complex.

Malicious Code – Software or firmware capable of performing an unauthorized function of an IS.

Malicious software code - Is any software code intentionally created or introduced into a computer system for the distinct purpose of causing harm or loss to the computer system, its data and resources. Many users equate malicious code to computer viruses, which can lie dormant for long periods of time until the computer system executes the trigger that invokes the virus to execute. Within the last several years, the Internet has been the conduit of various types of computer viruses. However, there are other types of malicious code used to cause havoc that are not as well publicized as the virus.

Mandatory Access Control (MAC) - Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity.

Metropolitan Area Network (MAN)- a loosely defined term generally understood to describe a broadband network covering an area larger than a local area network. It typically connects two or more local area networks, may operate at a higher speed, may cross-administrative boundaries, and may use multiple access methods. It may carry data, voice, video and image.

Manual cryptosystem
Cryptosystem in which the cryptographic processes are performed manually without the use of crypt-equipment or auto-manual devices.

Multilevel (security) mode
AIS security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:
a. Some users do not have a valid security clearance for all the information processed in the AIS.

b. All users have the proper security clearance and appropriate formal access approval for that information to which they have access.
c. All users have a valid need-to-know only for information to which they have access.

Multilevel security
Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

Need-to-know
Access to, or knowledge or possession of, specific information required to carry out official duties.

NETBUS – is a program used for remote administration or by a hacker to control a "target computer". The software consists of a server and client. The software is loaded via the Patch.exe file on the target computer by exploiting the Microsoft's Internet programs.

Network
Communications medium and all components attached to that medium whose function is the transfer of information. Components may include AIS, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Network Security - Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.

Non-communications emitter
Any device which radiates electromagnetic energy for purposes other than communicating (for example, radars, navigational aids, and laser range finders). A noncommunication emitter may include features normally associated with computers, in which case it must also meet the requirements for an AIS.

Password
Protected/private character string used to authenticate an identity or to authorize access to data.

PCMCIA – Personal Computer Memory Card International Association is an industry group organized in 1989. The group promoted the standards for a credit card size memory or I/O device that would fit into a personal computer.

Personal Computer
A personal computer normally a small desktop type AIS which contains an operating system, software applications, firmware, and storage devices (fixed and removable features) with the capabilities of operating, processing, and storing information in a stand-alone mode. PCs can be connected to networks for access to other systems.

NOTE: The category of personal computers can include lap-tops, notebooks and workstations.

Personal E-Mail Account
An E-mail account acquired by an individual for personal use. Also know as a private account.

Private Account
See Personal E-Mail Account.

Protected distribution system (PDS)
Wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Proxy Server - A type of firewall, proxy servers provide extra security by replacing calls to insecure systems subroutines. Proxy servers allow companies to provide World Wide Web access to selected people, by doing it through a network firewall.

Purge
Removal of data from an AIS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. See clearing.

RADIUS – Remote Authentication Dial-In User Service is a protocol by which users can have access to secure networks through a centrally managed server. RADIUS provides authentication for a variety of services, such as login, dial-back, SLIP, and PPP.

Remote terminal
A terminal which is not in the immediate vicinity of the AIS it accesses. This is usually associated with a mainframe environment and the use of a terminal. Terminals usually can not operate in a stand-alone mode.

Risk
The probability that a particular threat will exploit a particular vulnerability of an automated information system or telecommunications system.

Risk assessment
Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk management
Process concerned with the identification, measurement, control, and minimization of security risks in information systems.

Security Guard/Filter
AIS trusted subsystem that enforces security policy on the data that passes through it.

Security Test and Evaluation (ST&E)
Examination and analysis that the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of the system.

Small computer
A small general purpose computer designed to support a single user at a time. Disk drives, printers, and other equipment associated with the small computer are considered part of the small computer and normally referred to as a personal computer. In addition to the above standard definition and the changing mission of the Army, the definition of a small computer has been enhanced so that a small computer or any PC or workstation that attaches to a Server via a LAN in a client server environment is considered to be a small computer.

SPAM – unsolicited e-mail on the Internet, usually a form of bulk mail obtained from e-mail distribution lists or discussion group lists. The equivalent of unsolicited telemarketing phone calls except the email user pays for part of the message since everyone shares the cost of maintaining the Internet.

Stand alone computer
An automated information system that is physically and electrically isolated from all other automated information systems.

System Audit - Perform system audits and spot checks to verify secure operation of the system and support software. If irregularities are discovered, analyze and identify the problem and corrective actions necessary to resolve the situation. Explore all possible alternatives during the analysis. Actively track open items and brief management on identified security deficiencies.

Systems high (security) mode
AIS security mode of operation wherein each user, with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:
a. Valid security clearance for all information within an AIS.

b. Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs).
c. Valid need-to-know for some of the information contained within the AIS.

TACACS – Terminal Access Controller Access System. A system developed by the Defense Data Network community to control access to its Terminal Access Controllers (TACs).

Technical vulnerability
A hardware, firmware, communication, or software weakness which leaves a computer processing system open for potential exploitation or damage, either externally or internally, resulting in risk for the owner, user, or manager of the system.

Telecommunications
Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and automated information systems (security)
Protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats and to ensure authenticity. Note: Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information.

Telecommunications system
Any system which transmits, receives, or otherwise communicates information by electrical, electromagnetic, electro-mechanical, or electro-optical means. A telecommunications system may include features normally associated with computers, in which case it must also meet the requirements for an AIS.

TEMPEST
Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment (See compromising emanations).

Terminal
Any device which is used to access an AIS, including "dumb" terminals, which only function to access another AIS, as well as personal computers or other sophisticated AIS which may access other AIS as one of their functions.

Threat
Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to, information or an information system.

Threat agent
A means or method used to exploit a vulnerability in a system, operation, or facility.
Time Bomb and Logic Bomb - A time bomb is malicious code that can be triggered at a given time or date. The Michaelangelo Virus is an example of a virus containing a time bomb, which caused alarms in both the private, and U.S. Government computer systems several years ago. The logic bomb is triggered by an event instead of a specific time. One example of a logic bomb would be a programmer who creates a logic bomb to search the company's payroll files, checking for the presence of the programmer's name. When the programmer ceases employment, the logic bomb is triggered causing damage to data and software.

Transmission security
The component of COMSEC which consists of all measures designed to protect

transmissions from interception and exploitation by means other than cryptographic analysis.

Trapdoor - A trapdoor is a hidden software program (or can be embedded into the hardware or firmware) mechanism that causes the system protection mechanisms to be bypassed. The code can be hidden in the logon sequence where users are asked to input their user IDs and then passwords. In normal circumstances, the input passwords are checked against stored values corresponding to the user ID; if the passwords are valid, logon proceeds. The trapdoor software would check for a specific user ID, and whenever that user ID is checked, it bypasses the password checking routine and authorizes immediate logon. Trapdoors are sometimes built into development systems by programmers to avoid the lengthy logon procedure. However, they should all be removed once the system is deployed.

Trivial File Transfer Protocol TFTP) - A simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP), a connectionless protocol that, like TCP, runs on top of IP networks. It's used primarily for broadcasting messages over a network and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trojan horse - The Trojan Horse is malicious code created via the UNIX operating system. The UNIX operating system (and all other UNIX-like operating systems like LINUX) has a function called "SETUID" which can be manipulated by an experienced hacker to override read and/or write-protected files. For example, a mixture of public and sensitive information is contained in a database (DB). The DB is accessed by both the public and those users authorized to view the sensitive part of the DB via another file or computer program. A Trojan Horse can be created such that every time the unauthorized user (the general public in this example) accesses the initial file or computer program used to view the DB, instead of filtering out the sensitive information for viewing, the program is made to believe its the authorized user requesting access and treats the DB as if the requester has full access privileges. One can comprehend the enormous risk to an enterprise if, for example, personnel or sensitive information were accessed using a Trojan Horse.

UNTRUSTED NETWORK.

Unclassified but sensitive (SBU) information
Unclassified information, that the loss misuse or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

User
Person or process accessing an AIS by direct connections (e.g., via terminals) or indirect connections.

User ID
Unique symbol or character string that is used by an AIS to uniquely identify a specific user.

Virus
Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves not external signs of its presence.

Vulnerability
Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls), that could be exploited.

Vulnerabilities - Systematic examination of an IS or product to determine the adequacy of security measures, identify security

deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Wide area network (WAN) – Commercial examples are Internet, and Public data. Government examples are NIPRNET and SIPRNET. A WAN covers a wider geographic coverage than a LAN, is an integrated voice/data network, often uses common carrier lines interconnection of LANs, and consists of nodes connected over point-to-point channels

World Wide Web - Also called WEB or W3. The World Wide Web is the universe of accessible information available on many computers spread through the world and attached to that gigantic computer network called the Internet. The Web has a body of software, a set of protocols and a set of defined conventions for getting at the information on the Web. The Web uses hypertext and multimedia techniques to make the web easy for anyone to roam, browse and contribute to. The Web makes publishing information (i.e. making that information public) as easy as creating a "homepage" and posting it on a server somewhere in the Internet. Pick up any Web access software (e.g. Netscape), connect yourself to the Internet (through any of the dial-up, for-money, Internet access providers or to one of the many free terminals in Universities) and you can discover an amazing diversity of information on the Web.

Worm - An independent program that reproduces by copying itself from one system to another, usually over a network. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources and even shutting down a network.